Relationship and Cloud Factors Affecting Government Confidence in the Public Cloud

PhD Thesis

WALEED IBRAHIM AL-GHANIM

This thesis is submitted in partial fulfilment of the

requirements for the degree of Doctor of Philosophy

Software Technology Research Laboratory

De Montfort University

United Kingdom

May 2017

ACKNOWLEDGEMENTS

First and foremost, I want to thank Almighty Allah for His favours and guidance. Secondly, I would like to offer my sincere appreciation to my supervisor Dr. Feng Chen, for his invaluable guidance, support and encouragement and without him the research would not be possible. I would also like to express my thanks for my second supervisor Dr. Martin Ward for his valuable comments, suggestions and support. A heartfelt thanks to the staff at De Montfort University, in particular the staff at STRL for their support, and to my colleagues for the support and advice. I would also like to thank the Saudi Customs Department and the Government of Saudi Arabia for allowing me the opportunity to study in the United Kingdom.

I would like to express my love and appreciation to my mother and father for their prayers and support. I also would like to express my deep thanks to my beloved wife for her prayers, patience, understanding and support throughout my research. Last but not least, I would like to thank my children for their patience and support during our time in the United Kingdom.

ABSTRACT

Despite the advantages of the public cloud governments are still reluctant to deploy sensitive data and critical systems into the public cloud. The advantages of scalability and cost are attractive for governments and the current trend is for governments to consider placing more of their data and systems in the public cloud towards a more comprehensive government cloud solution. However, there are major concerns related to the public cloud that are especially significant to governments which are cause of reluctance in terms of public cloud adoption. Such concerns include security and privacy, governance, compliance, and performance. If these concerns are answered, governments will perceive less risk and be more confident to deploy to the public cloud. Besides the obvious technical solutions, which include improving security, another solution is an effective cloud service provider (CSP) - government relationship.

Towards the development of such a solution the study contributes a novel approach to researching the CSP-government relationship in order to reveal, in depth and comprehensively, the relevant relationship and associated cloud issues, often neglected in previous research. Specifically, the developed research design was achieved through a mixed methods approach using a questionnaire and semi-structured interviews with senior IT professionals in various government ministries and departments in Saudi Arabia.

The findings not only offer a comprehensive and in-depth understanding of the relationship, but also reveal specific relationship and cloud issues as problems towards the development of a solution to increase government confidence in the public cloud. Specifically, it was found that government were more concerned about areas of the cloud that are more relevant to government and there was often an associate lack of trust or perception of risk for these areas. Moreover, it was found that in relation to more specific areas of the cloud there was increasing concern in terms of trust and risk, the ability to negotiate and collaborate, and the perception of reputation.

Based on these findings, which also revealed the various interplays between relationship factors as a novel contribution, the study offers recommendations to CSPs on how they may improve their relationship with the government. This is to be achieved through resolving relationship issues and associated cloud concerns within the relationship context towards improving government confidence in the public cloud. The findings also have implications for other parties which include governments considering the public cloud and those engaged in academic research in the area of government reluctance to use the public cloud.

PUBLICATIONS

Conference

- Attended the Third International Conference on Advances in Information Processing and Communication Technology – IPCT' 15 10 -11 December 2015 – Rome, Italy. Presented and published paper.
- Attended the Fifth International Conference on Advances in Computing, Electronics and Electrical Technology – CEET' 16, 12 -13 March 2016 – Kuala Lumpur, Malaysia. Presented and published paper.
- Attended the Fourth International Conference on Advances in Information Processing and Communication Technology – CCIT' 16, 17 -18 March 2016 – Birmingham, UK. Presented and published paper.
- Attended the Fourth International Conference on Advances in Computing, Electronics and Communication – ACEC' 16, 15-16 December 2016 – Rome, Italy. Presented and published paper.

Journal

- Alghanim, W. and Chen, F. (2016). Suitability of Frameworks, Standards and Certification for Government Adoption of the Public Cloud For Advance Digital Continuity. International Journal of Research in Science and Technology. 6 (III), 14-24.
- Alghanim, W. and Chen, F. (2016). A Relationship Approach to Increasing Government Confidence in the Public Cloud for Sensitive Data Deployment. International Journal of Research in Science and Technology. 6 (III), 25-36.
- Alghanim, W. and Chen, F. (2016). Building Public Confidence in the Public Cloud through Improved SLAs. International Journal of Research in Science and Technology. 6 (III), 37-43.

- Alghanim, W. and Chen, F. (2017). Relationship and Cloud Factors Affecting Government Confidence in The Public Cloud. International Journal of Research In Science & Technology. 7 (1), 1-8.

Poster

- Attended 8th Saudi Student Conference in London, 31st January until 1st February 2015. In this conference, I presented a poster of my research.
- The 6th PhD Experience Conference in Hull 7th to 8th April, 2015. Poster presentation.
- Attended 9th Saudi Student Conference at University of Birmingham, 13 - 14 February, 2016. Poster presentation.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

PCC	Public Cloud Computing
CSP	Cloud Service Provider
CP	Cloud Provider
CC	Cloud Customer
SP	Service Provider
IT	Information Technology
SLA	Service Level Agreement
IS	Information Systems
CSFs	Critical Success Factors
CCSFs	Cloud Critical Success Factors
EU	European Union
US	United States
ENISA	European Network and Information Security Agency
EC	European Community
VDES	Virtual Data Embassy Solution
ICT	Information Communication Technology
TOE	Technology Organisation Environment
QoS	Quality of Service
AUPs	Acceptable Use Policies
TM	Trust Management
RCSFs	Relationship Critical Success Factors
PMT	Protection Motivation Theory

1 Introduction

Objectives

- **Give an introduction and the motivation of this research**
- **Introduce aims and objectives**
- **Present the research methodology**
- **Present the thesis structure**

1.1 Research Motivations

Often governments when using cloud solutions will use private clouds whereby the cloud infrastructure is physically located within their borders or within their embassies in other countries. In terms of security this offers benefits because they can implement their own firewalls and the IT departments have direct control over the data. This security is particularly important because governments use sensitive data and critical systems, as well as non-sensitive data, in the cloud for e-government and backup and disaster recovery purposes.

The control, or governance, over data and systems is important for governments who must be compliant with laws and regulations that require a certain level of control. Where governments do use public clouds, the benefits of which include cost, scalability and portability, there are security and governance issues and often only non-sensitive data and non-critical systems are put in the public cloud. However, it is important that governments use public clouds as part of an overall cloud solution to take advantage of the benefits of the public cloud. Due to such advantages, the future direction of government in the cloud will involve the use of the public cloud.

Not only does the public cloud have advantages in terms of cost and scalability, but in the case where a country wants to ensure that there is digital continuity where their physical infrastructure, which supports their private cloud, is compromised, then they need to look at a public cloud solution whereby data and systems are stored in multiple virtual locations around the world as part of the overall solution. This will ensure that a government can continue to function in the public cloud and provide services to its citizens even in the event that their territory is compromised. An example of this is Estonia, a country that is concerned about a threat to its territory from Russia as well as cyber warfare and is working with Microsoft to provide such a ‘virtual data embassy’ solution where all its e-government systems will be virtualised in the public cloud.

It is accepted that governments have cloud-specific concerns which include security and privacy, governance and compliance as well as customised service and performance offerings, all of which impede willingness to use the public cloud. Governments are reluctant to place sensitive data and critical systems in the cloud because they do not have confidence in these cloud-related areas as well as receiving specialised and customised services that they

need. In relation to the latter point, due to the nature of the public cloud service offerings are often standard which are not suitable for governments.

In addition to the aforementioned cloud concerns, there are relationship issues that also impede willingness to adopt the pubic cloud, the most notable of which include trust in the cloud service provider (CSP), associated perceptions of risk, the ability to negotiate requirements, the ability to collaborate and the perceived reputation of the cloud services. Therefore, consideration of a relationship within which reluctance or otherwise to adopt the public cloud may occur, would require consideration of both cloud and relationship factors towards understanding such reluctance.

However, particular consideration of both these types of factors in combination is either rare or weak in the literature. Studies often consider either cloud-related factors (Bhatt, 2012, Aziz et al., 2013, Ahmad and Janczewski, 2011, Lecklider 2014, Trigueros-Preciado et al., 2013) or relationship-related factors (Wang and Wu 2014) in isolation or there is little attention paid to the links between the two or the fact that they exist together (Filali and Yagoubi, 2015, Hana 2013, Alshomrani and Qamar 2013, Almorsy 2011, Fan et al. 2014, Ding et al. 2014). Studies merely mention factors without considering a connection between them. This study builds on this and investigates the links in detail to provide a better understanding of this dynamic.

The motivation behind this study is to reveal concerns in the government-CSP relationship by considering both relationship and cloud factors in combination. It would be not enough to say, for example, that governments are concerned about compliance, rather it is necessary to reveal the relationship reasons why they are concerned about compliance, for example because they do not trust the CSP in relation to compliance, or they feel they are unable to negotiate compliance requirements.

In support of a relationship approach to the problem of reluctance to adopt the public cloud, the European Union Agency for Network and Information Security (ENISA) say there are two possible solutions to these concerns; firstly, the development of technology that would serve to alleviate these concerns such as improved security, and secondly, an improved relationship between government and the CSP where governments can negotiate and collaborate for the cloud service that they require and trust can be achieved (ENISA, 2015).

In pursuit of these ideas, the study offers a research design that investigates the relationship from both the cloud and relationship factor perspectives, revealing the links between them in order to offer a more comprehensive and more detailed understanding of the relationship and the specific areas of concern that may cause reluctance to adopt the public cloud. The research is carried out with government organisations in Saudi Arabia as a case study, this includes the Ministry of Finance, Saudi Customs, Saudi Immigration and the National Information Centre.

1.2 Research Problem

The reluctance of governments to use the public cloud is related to the perception of risk and the level of trust that they have in the CSP, and the negotiation and collaboration that takes place between the two parties. Therefore, there is a need to examine the relationship in order to find out factors related to that relationship and cloud requirements that may be impeding government confidence to use the cloud. Other studies that have addressed this relationship have been limited in that they only examine the cloud related factors such a governance or security and privacy, or they only examine relationship factors and the links between the two are often weak. Therefore, there is a need to overcome this limitation by considering relationship and cloud factors and the links between them in the context of the cloud provider – customer relationship.

Overall, it is important to remember that governments have specific and unique needs from the public cloud and that it is in the relationship where confidence or otherwise is attained for the cloud related factors. This study expands on other studies where cloud concerns or relationship concerns are addressed in isolation. Not only does this study reveal the relationship concerns of government but also how those relationship concerns are related to aspects of the cloud, such as governance or security and privacy, and how this has an impact on the confidence to adopt the public cloud.

Government reluctance to adopt the public cloud is something that affects governments globally. There is variation in the extent of progress towards public cloud adoption. Such variation ranges from the example of Estonia where real intention and progress for government in the public cloud exists, evidenced by a joint project with Microsoft which is currently assessing the feasibility of moving government to the cloud, to countries of the European Union, including the United Kingdom where there is consideration of the public

cloud on a limited and controlled basis, to finally, developing countries such as those in the Gulf region, including Saudi Arabia, where there is significant reluctance as well as understanding of the benefits of the public cloud for government. In fact, consideration of the public cloud in the Gulf region is something that is taking place, however, there are concerns about the development of technology especially in terms of security and privacy. In Saudi Arabia in particular, the reasons that have been put forward about government reluctance include business, financial and technical reasons and economic reasons but no mention of the relationship with CSPs. There is a real need for consideration of adoption of the public cloud in the region, this includes economic benefits and specifically to support the emergence of smart cities, however, the interest until now has only come from the private sector because there is a real concern about data being stored outside the country. Despite this, the government of Saudi Arabia has been introducing regulation for the public cloud in the country, therefore, there is an interest in the public cloud and an associated need for government to achieve what they need from the CSP. Despite the fact that there is variation in terms of the level of progress in different countries, there is still overall reluctance that needs to be addressed through the CSP – government relationship.

1.3 Research Questions

1. What are the relationship and cloud factors relevant to the government – CSP relationship?

2. Do relationship related factors and cloud factors affect each other which could affect government confidence in the public cloud?

The first research question relates to the idea that there are a number of relationship and cloud factors that are relevant to government that need to be identified first before the relationship can be investigated. The second research question is about the interplay between relationship and cloud factors that could affect confidence in the public cloud.

In order to answer the research questions the following aims and objectives are established for the study:

1.4 Aims and Objectives

Based on answering the research questions, the study establishes the following aims and objectives. The aims are what the study intends to investigate, and the objectives how these aims will be achieved.

1.4.1 Aims

- To reveal issues about relationship and associated cloud factors in the government – Cloud Service Provider (CSP) relationship.
- To determine specific areas of concern within the government - CSP relationship that includes relationship and associated cloud related factors that may have an effect on government reluctance to adopt the public cloud.

1.4.2 Objectives

- To research the specific relationship and cloud factors in the government - CSP relationship.
- To reveal the links between the relationship factors and cloud factors in the government - CSP relationship.
- To develop and apply a research design that combines these relationship and cloud factors to better understand government reluctance to adopt the public cloud.
- To provide recommendations on how the government-CSP relationship can be improved towards decreasing government reluctance to adopt the public cloud.

1.5 Scope of Research

The research is being conducted with the government of Saudi Arabia because it is a country that is currently using the public cloud on a limited basis and does not use it for sensitive data and critical systems. The government have expressed concern and reluctance for using the public cloud in this way, however, it has been shown in the literature that eventually to take advantage of the public cloud fully, the government will have to migrate more of its services to the public cloud as part of government trends globally in this area.

Primarily, the study reveals the relationship and cloud issues towards understanding the reluctance of governments to utilise the public cloud for sensitive data and critical systems which is the next inevitable step in cloud computing for governments. The scope of the

research includes the relationship between the Saudi government and the CSP which includes the relationship where terms are negotiated and agreed and collaboration during the working relationship between the two parties. Relationship factors also include trust, the perception of risk and reputation. All of the relationship factors used in the study have been identified as the relevant factors in the relationship between government and CSP from the literature.

Moreover, the scope of the research includes cloud factors which again have been identified from the literature. In the identification of cloud factors there was careful consideration of cloud factors that would be relevant to government, and although these include concerns that all types of organisation would have, cloud factors that are particularly important to government, such as governance over data and compliance with laws and regulations, are also included. Specifically, the cloud factors included governance, compliance, security and privacy and performance and offering. Any concerns that the government would have about the cloud can be found within these four areas. However, these cloud factors are broad and clearly incorporate numerous aspects within each. Therefore, as part of the development of the research design of the study, areas (sub cloud factors) within each cloud factor are identified, again, as being relevant to government. To provide an example, within the governance cloud factor a sub cloud factor was '*control and knowledge of CSP employees*' which for a government is particularly important as there may be spies or saboteurs from other countries employed by the CSP. The sub cloud factors also included factors that would be of concern to both government and other types of organisation such as private enterprise, and examples include auditing and measuring the CSPs performance and clarity of roles and responsibilities.

This study contributes to understanding the possible reasons why government does not have the confidence to use the public cloud, but it does not investigate the direct link between cloud and relationship factors on the one hand and lack of confidence on the other. Therefore, the scope includes revealing issues within the government - CSP relationship that may have an effect on confidence, however, the actual link between relationship and cloud factors and confidence is a subject for future study.

1.6 Research Design

The study is about investigating the relationship factors and associated cloud factors that can have an effect on government's confidence to adopt the public cloud. Thus, the research

design of the study considers relationship factors that are relevant to this relationship and include trust, risk, collaboration, negotiation and reputation. The study aims to investigate the areas of the cloud itself where the relationship factors would have an impact, these areas are the relevant areas that governments would be concerned about when considering the public cloud and include governance, compliance, security and privacy and performance and offering which are also considered in the research design.

The research design is intended to show how relationship factors are linked to cloud factors, for example where a government does not trust (relationship factor) the governance structures (cloud factor) offered by a cloud provider, is an area of concern. Moreover, the study offers greater insight by considering the specific issues within each cloud factor, namely; the sub cloud factors, for example, where governance is the cloud factor; control over data would be a cloud sub factor.

All factors, whether relationship, cloud or cloud sub factors are considered in the study as critical success factors for government confidence in the public cloud. These factors form the basis of the development of the methods which include a questionnaire and a semi-structured interview.

1.7 Research Methods

Based on a research design which considers both relationship and cloud factors together, a mixed methods approach was used, including a quantitative questionnaire and a qualitative semi-structured interview. This approach was adopted because both relationship-specific and cloud-specific CSFs are already known in the literature, but the study wanted to find out specific issues within the relationship which factors were significant in terms of affecting government confidence in the public cloud. The questionnaire served this purpose through identifying which cloud-specific CSFs, such as governance, are there issues of trust, risk perception, negotiation and the services offered. However, the study does not assume to know everything about the relationship that could affect government confidence in the public cloud, and therefore, a semi-structured interview was adopted to reveal concerns that governments have in relation to the relationship-specific factors and the cloud-specific factors. The participants in the study included government personnel from the Ministry of Finance, Saudi Customs, Saudi Immigration and the National Information Centre, who are involved in the negation with cloud service providers.

1.8 Contribution

There are numerous studies that have addressed the concerns associated with adopting the cloud (Bhatt, 2012; Diez and Silva, 2013; Aziz et al., 2013; Almorsy, 2011; Ahmad and Janczewski, 2011; DiModica, 2014; Alshomrani and Qamar, 2013; Zwattendorfer et al., 2013; Tripathi and Parihar, 2011; Haag et al., 2014; Nycz and Polkowski, 2015; Brenda and Markov, 2013). These studies either consider cloud concerns such as security in isolation or where they do consider relationship factors a simple link is made, for example, customers do not trust the CSP for security. These studies are limited in that they simply state there is, for example, a perception of risk for governance or a lack of trust in security technology. There is a lack of a more detailed understanding of these issues, which clearly include a relationship factor such as risk and trust and a cloud factor such as security or governance, within the relationship context. It is within the relationship between the cloud customer, in this case the government, and the CSP, where confidence in the public cloud can be achieved.

In order to understand the issues, that may cause reluctance for the public cloud, that may occur in the relationship context it is important to consider the cloud concerns and the relationship concerns that feature in that context. However, these concerns do not take place in isolation, and although there are studies that do consider them together, the link is weak, or the study is too broad, or no detail is considered. Importantly, studies do not consider all relevant relationship and cloud factors within a relationship context, whereby the relationship is considered a major solution to alleviate reluctance about the public cloud. Therefore, if there is a need to understand the relationship in more detail, all the relevant relationship and cloud factors need to be considered together, something that has not been done until now.

This study applies these ideas through the development of a research design which is applied in the form of a questionnaire. This is another contribution of the study that can be applied in different government-CSP relationship contexts.

Through the application of the research design the study offers a detailed insight and understanding of the issues that cause government reluctance, or even confidence, to adopt the public cloud for sensitive data.

In light of the fact that the abovementioned contribution of the study is to reveal the issues within the relationship and offer a greater insight into that relationship, this leads to another contribution of the study which is offer recommendations as solutions to the identified

problems. Specifically, recommendations are offered to the CSPs on what they can do to increase government confidence in the public cloud.

Below is a summarisation of these contributions:

1. A new approach to consider the relationship between the government and CSP that considers all relevant relationship and cloud factors together.

2. The development of a research design that is developed to reveal relationship and cloud factors in the relationship context and the various connections between them.

3. The development of a research instrument that can be applied to different government-CSP relationships.

4. A deeper insight and understanding of the issues in the government-CSP relationship and the associated reluctance to adopt the public cloud.

5. Recommendations on how to improve the government-CSP relationship and increase government confidence in the public cloud.

1.9 Success Criteria

The following are the success criteria for the study:

- Identification of relationship and cloud related issues in the government-CSP.
- Identification of the associations between relationship and cloud factors.
- Successful application of developed research design.
- Identification of potential issues that may affect cloud adoption.
- Development of recommendations based on analysis.

1.10 Thesis Outline

Chapter 2 – presents a review of the literature related to the cloud in general, e-government, associated issues related to governance, security, sensitive data and legality and regulation. The review also presents models of adoption for the cloud and the associated issues of trust and risk perception.

Chapter 3 – This chapter explains the research design of the study. Specifically, there is an explanation of how the research considers and combines relationship and cloud related factors towards a deeper understanding of the reasons for government reluctance for adopting the public cloud.

Chapter 4 – This chapter presents the methodology for the study. Specifically, the methodological approach and the adopted methods are explained and justified.

Chapter 5 – Presents the results and analysis of the questionnaires.

Chapter 6 – Presents the results and analysis of the interviews.

Chapter 7 – Discussion of the findings of the study and the implications the findings have in relation to other studies.

Chapter 8 – This chapter concludes the study, shows the contributions and implications of the work, identifies the study's limitations and makes recommendations for future study.

2 Background and Literature Review

Objectives

- **Review literature about relationship factors**
- **Review literature about cloud factors**
- **Review literature about government and the cloud and associated concerns**
- **Review existing literature about trust in the cloud**
- **Identify research gaps**

2.1 Overview

A review of the literature was conducted to identify and perform an analysis of the literature that is relevant to the government – CSP relationship in the context of public cloud adoption. Moreover, the review of the literature will reveal the gaps in the research which will support the rationale for the study. Moreover, the present study is established on an approach to researching the government – CSP relationship which is partly developed based on the work of other authors in addition to models for cloud adoption. The sources that are used in this literature review include books, journal articles, models, government publications and news media. Government websites of the government of Saudi Arabia were also used in order to research the latest developments and possible issues related to government adoption of the cloud.

2.1.1 Search Method

The researcher was interested in literature that was related to cloud computing, the associated issues of cloud computing, reasons for reluctance for cloud adoption, issues in the relationship between cloud provider and cloud customer, government in the cloud and the future of government in the public cloud. The search included use of the university database to identify academic journal articles, conference papers and news and magazine articles.

2.2 Key Concepts

Here the key concepts on which the study is based are presented. These concepts relate to issues that directly affect governments' adoption of the public cloud for sensitive data as part of an overall government cloud solution.

2.2.1 Security and Privacy

Despite the numerous benefits of governments using the cloud which includes cost savings there still needs to be consideration of the challenges of adopting cloud technology (Bhatt, 2012, Diez and Silva, 2013, Aziz et al., 2013). The main concerns of governments using the cloud are related to security and privacy, especially that related to sensitive data. The general idea is that sensitive data is for the private cloud and non-sensitive data in the public cloud (Bhatt, 2012, Khan et al. 2011, Lecklider, 2014, Diez and Silva, 2013).

In addition to the security concerns associated with loss of governance the characteristics of the cloud present other security concerns. These issues relate to shared resources, multiple tenancies, third party hosting and multiple access points. Multiple points of vulnerability increase the risk of the system being compromised. In relation to the above-mentioned issues, there is a need for improved cooperation between cloud vendors and governments to create unified global rules for safer government clouds (Liang, 2012).

2.2.2 Governance

The nature of the public cloud means there is a loss of governance by the owner of the data unlike with private clouds. Moreover, the security itself is a service provided by the cloud provider and is not in the hands of the government, this is especially a problem because there is a shift in the responsibility of governance and control.

There is also the issue that there are multiple parties involved in the situation, there is the cloud provider, the cloud service provider, there are many different employees in each of these organisations and there are multiple tenants who share the cloud. These factors, each pose risk in terms of governance and security and privacy of government data. Each party has their own security requirements which may conflict (Almorsy, 2011).

Governments require a certain level of control over their data and systems. This control, or governance, may be in the form of direct control over data or may be simply being informed of the location of data.

2.2.3 Compliance

With a public cloud solution for e-government, the servers which are used will be located outside of the sovereign territory of a country which gives rise to legal concerns about citizen data being located in another jurisdiction and the laws of the jurisdiction which may allow another country to subpoena the data for investigatory purposes (Ahmad and Janczewski, 2011). In order to resolve these problems governments would have to make changes to domestic laws, but only if the benefits of using the public cloud outweighed the risks (ENISA, 2011). In 2015, the European Union Agency for Network and Information Security (ENISA) says that the solution to this issue lies in the relationship between government and cloud providers.

Legal issues are also relevant to the cloud provider, where it may not be possible for the cloud provider to comply with the law and auditing requirements of a government customer because of the laws of their own jurisdiction or they may not have the ability to do so because the nature of the public cloud and its benefits means that cloud service providers can only offer generic SLAs to its customers (Ahmad and Janczewski 2011).

2.2.4 Service Provision

Due to the nature of the public cloud it is often the case that service offerings are standard, DiModica (2014) says that standardised offering is a problem and it does not allow those who wish to pay for a differentiated service which is often the result of an inflexible negotiation. The solution to this problem has been the idea of some form of dynamism in the SLA. Kanwal (2015) puts forward the idea of the need to have active agreements that are updated periodically and Filali and Yagoubi (2015) put forward the idea of a dynamic SLA. This is especially the case with governments who not only require a tailored solution in the public cloud, but they also need a dynamic SLA. A dynamic SLA will serve two purposes, firstly, it will be flexible enough to adapt to the changing requirements that governments will have, and secondly, it will also allow governments to monitor the SLA against performance requirements and adjust accordingly.

2.2.5 The future of government in the public cloud

A pioneering project to place e-government into the public cloud has been initiated by the government of Estonia, who with the help of Microsoft has embarked on a project to test the viability of placing sensitive data and critical systems into the public cloud. Estonia is under threat from Russia both territorially and through cyber-attacks and part of its strategy has been to create private clouds in physical Embassies in friendly countries around the world, while there are security advantages to this solution, these private clouds can still be vulnerable to cyber and physical attack. A development of their strategy has been using ‘Virtual Data Embassies’ in the public cloud. Specifically, the project involved placing the President’s website and the government gazette into public clouds around the world as a test towards the ultimate solution of virtualizing all government services in the public cloud so that the government can continue to provide e-services to its citizens even in the event that its physical territory and IT/IS infrastructure is compromised.

Such an endeavor would require overcoming the limitations of the public cloud through a special relationship with the cloud provider, especially in the area of governance where governments would need more control in order to comply with laws related to the security and privacy of sensitive government data. Although in the Estonia project the country is working directly alongside the public cloud provider, Microsoft (Microsoft Azure cloud solution), the project highlights the security and privacy issues in the public cloud and how this relates to the relationship between the government as a customer and the public cloud provider and the Service Level Agreement (SLA) towards the possibility of other governments considering using the public cloud for sensitive data and critical systems on a permanent basis.

2.2.6 Relationship Factors

During any negotiation for the acquisition of information technology, there is a level of perception of risk and the purchaser much have a certain level of trust in the provider. Moreover, there needs to be an effective relationship between the two parties where the buyer is able to effectively specify their requirements and the provider is able to understand these requirements. These factors, together with the services that are offered and the reputation of the supplier service to affect both trust and perception of risk. These ideas are particularly relevant to the issue of collaboration between the two parties. In this study theories and ideas about risk, trust and collaboration are considered. It is important to consider these factors in a study that seeks to establish the reasons related to the relationship that are causing a lack of confidence in the public cloud. Theories considered include Protection Motivation Theory, which says that organisations will protect themselves when they perceive a risk and will avoid negative consequences if they have the ability to carry out preventative measures and Risk Compensation theory says that more risk will be taken if there is an increased level of security (Huntgeburth, 2015).

2.3 Government in the Cloud – Challenges and Benefits

Governments want to improve the performance of the public sector through the use of cloud technology (Bhatt, 2012) and they are under pressure from decreasing IT budgets and increasing demands for their services and that a solution to this problem is cloud computing (Diez and Silva, 2013).

There are a number of commonly accepted benefits of using the cloud which includes cost reduction, according to the United States government where the government moves to the cloud millions of dollars are saved; these cost savings are from the fact that there is no need to invest in building and maintaining infrastructure (Department of Defense, 2012). The idea of cost saving is echoed by Khan et al. (2011) who bring attention to the economic benefits which include the fact that only the resources that are used are paid for and that traditional IT administration costs are almost completely removed, the financial benefits which includes saving on capital costs which are replaced by operational costs and finally, timeliness, whereby resources can be obtained in a matter of hours which is sharp contrast to the time takes to install in-house computing resources. Similarly, Chandra and Bhadoria (2012) say that the benefits of the cloud include lower costs, the shift of capital expenditure to operating expenditure, agility, dynamic scalability and simplified maintenance.

Speed and flexibility is another common benefit where the cloud offers flexible solutions which include that services can be scaled up or scaled down and increased security is another commonly accepted benefit of the cloud. The best of the cloud service providers offer state of the art of security where data is often hosted in physically secure data centres (Department of Defense, 2012). In reference to benefits, Bo (2013) approaches the issue of e-government in the cloud from the angle of data storage and says that a cloud solution solves the problems that governments have with storing large amounts of data.

Khan et al. (2011) say that the benefits of the cloud include on-demand self-sufficient services, location independent resources, ubiquitous network access and rapid elasticity. Additional benefits include that cloud computing allows leapfrogging opportunities for lesser developed countries to develop (Khan et al. 2011).

Diez and Silva (2013) say although public organisations face similar challenges to private organisations, the fact that public organisations offer different types of service such as social interaction and open data it means that cloud computing is a more attractive option. However, the uptake of the cloud has been less for public organisations due to the challenges which include a lack of established standards and the fact that there are not enough cloud providers who meet government requirements; this makes the provision of cloud services to public organisations less attractive for cloud providers because of these legal and regulatory requirements (Diez and Silva, 2013). Hana (2013) says that the benefits of the cloud for governments are encountered by a number of difficulties which include security, privacy,

performance and reliability, in addition to concerns about the law and national and international regulatory framework.

Aziz et al. (2013) focus on the challenges of adopting cloud technology for E-government and say that although it has many benefits, one of them is cost savings, they bring attention to the fact the due to the technology itself, there are also risks and importantly that the success of the implementation of this technology depends on how well the government deals with the challenges. Therefore, governments need to be careful about E-government adoption because if not it could result in damage to the reputation of public administration, decrease in customer satisfaction and financial loss (Aziz et al., 2013).

Aziz et al. (2013) further say that the potential of cloud computing for E-government is something that still needs to be explored as it is a continuous process; they encourage further research into the advantages and disadvantages in order to weigh up the benefits of cloud technology for government. Alshomrani and Qamar (2013) also address the challenges and benefits of the adoption of cloud computing by E-governments and Bhatt (2012) also considers the advantages, limitations, problems and solutions of cloud computing for E-government and the emerging future trends. Diez and Silva (2013) looks at the impacts and benefits of cloud computing for the public sector and an interesting question that is raised by these authors is why have few public organisations adopted cloud computing as it has been successful and widely accepted by other types of organisation?

Thus, despite the benefits, there are a number of challenges when deploying the cloud for the government sector. Zwattendorfer et al. (2013) say that these challenges include security and privacy concerns with sensitive data in the cloud, compliance, interoperability and portability, identity and access management and auditing. Tripathi and Parihar (2011) present technical, economic and social challenges. Under the technical challenges Tripathi and Parihar (2011) talk about legacy systems, some of which can be written into the new cloud computing environment, but for some that could be too expensive and thus a key factor is the interoperability between existing software and hardware platforms. The economic challenge is mainly related to return on investment and weighing up the costs against the benefits. Social challenges are related to the usage, accessibility and acceptance.

2.3.1 Governance

Haag et al. (2014) says that in addition to the challenges of cloud adoption by the government which includes security, transparency and accountability there is also the impact on IT governance. Governance is a specific issue that is especially a concern for governments where opting for the public cloud mean that governments lose control over their data. Nycz and Polkowski (2015) acknowledge that the governance issue in cloud computing is the lack of physical control of the data. In reference to this lack of governance in the public cloud, Diez and Silva (2013) say that the lack of control of cloud services and not knowing how cloud systems are managed by the cloud providers is a cause for concern, they say that although the government is the owner of the data, the cloud provider is the custodian and thus, the cloud provider has to meet the data owner's security requirements. Nycz and Polkowski (2015) echoes these concerns and say that the main problem with cloud computing is the lack of physical control of the data. An important point related to governance was raised by Abbadi and Alawneh (2012) who said that users should have the ability to control their data in the public cloud.

Brenda and Markov (2013) say that the loss of governance over the IT infrastructure is a major risk of cloud computing. Particularly, this loss of governance can lead to problems related to regulatory compliance. Another problem that is associated with the issue of governance is that the risks associated with the cloud are often dealt with in agreements, this is in contrast to internal IT governance (Yigitbasioglu, 2015) therefore, the problem lies in the fact that risks are not managed through governance mechanisms.

The main difference between normal IT systems and cloud computing in terms of security is governance, in that the organisation loses control over assets and information, this means that the collaboration between the cloud provider and the customer is essential in order to reduce the threats associated with loss of governance by the customer (Rebollo et al., 2012). Moreover, because of the continuously changing nature of cloud computing there is a need for an assurance framework in order to secure the cloud model and a clear governance strategy to be developed in order for enterprises to benefit from cloud computing (Rebollo et al., 2012). According to Craig et al. (2009) the public sector will face challenges in relation to governance when they adopt cloud computing, governance here is referred to as that related to compliance with legal and policy constraints and internal and external auditing requirements. The problem of governance is made worse by geographical dispersion,

problems include enforcement difficulties, increased monitoring costs and ensuring rights when data are stored overseas (Craig et al. 2009).

The governance risks in the cloud are similar to those faced with any outsourcing of IT. One of the ways that governance, risk can be mitigated is through effective contractual arrangements which can be assured through an effective SLA. The issue of governance for government in the cloud has a great influence on decisions for risk management, this is mainly due to large concentrations of data and resources that are in the cloud (Elena, 2013) which include the outsourcing of key organisational processes. The link between IT governance and risks has been identified by Yigitbasioglu (2015) who says that IT governance needs to be developed in order to mitigate risks and mitigating risks will in turn improve IT governance.

In reference to Saudi Arabia the loss of governance has been cited as one of the significant reasons for the Saudi public sector opting for a private cloud solution, because governance requirements of the government cannot be met by the public cloud (Mreea and Munasinghe, 2016).

Because sensitive data is process outside of an organisation there is a bypass of the logical, physical and personnel controls that IT staff exert over in-house programs (Elena, 2012). However, customers of the cloud are responsible for their own data, but they do not know where their data is hosted and how the cloud environment where the data is hosted is used by other customers (Elena, 2012).

2.3.2 Security Issues

Although the advantages of e-government using the cloud are clear, there are serious security and privacy issues, which ENISA (European Network and Information Security Agency) say are ‘show-stoppers’ for the adoption of the cloud (Luna et al, 2011). Security is one of the most significant issues when it comes to the adoption of the cloud by e-government and has been the main reason for the reluctance for adoption by government. The reason for such concerns is obvious; e-government data contains highly sensitive data about citizens. Clouds are susceptible to hacking, not only for data that is stored but also for data that is transmitted (Bhatt, 2012).

According to Spiga et al. (2014) threats to security is the main barrier for full adoption of cloud computing, despite the benefits of the cloud, this is especially the case for public

administrations because security is more critical, therefore, there needs to be consideration of security and privacy laws in the development of the delivery model. Ahmed and Hossain (2014) say that unless security is consistent and robust there will be little credibility in the advantages that cloud computing has to offer.

Security is essential in the government sector and has to be provided in several layers, these include the network, applications and the data security (Zwattendorfer et al., 2013). Similarly, Hashizume et al. (2013) say that cloud computing is a new computing model and there is uncertainty about security at different levels, which include the host, the network, data and applications, for the latter there is a concern of how application security is moved to the cloud.

Security concerns are related to risk areas which include dependency on a 'public' internet, data storage, multi-tenancy, lack of control (governance) and therefore, traditional security measures which include authentication, authorisation and identity are now not enough for the cloud (Hashizume et al. 2013). Moreover, there is a need to objectively and quantitatively measure security of services offered by a cloud service provider (Luna et al, 2011). Although security controls in cloud computing are no different to security controls in any IT environment, because of the operational models that are employed and the technology that is used, cloud computing presents different risks (Hashizume et al. 2013).

Anitha (2013) say that due to the fact that there are a number of different technologies used in the cloud which includes transaction management, virtualization, resource allocation, databases, cloud networks and operating systems, Anitha (2013) summaries the security issues that are faced by cloud computing as follows:

1. Data access control: this refers to the illegal accessing of data because of a lack of secured data access control, this is especially a problem for sensitive data stored in the cloud.
2. Data integrity: problems related to data integrity can arise from human error when data is inputted or hardware malfunctions, this is relevant to the cloud because there are many people accessing and managing the data.
3. Data theft: because the cloud uses external servers they are more exposed to theft
4. Data loss: considered a serious problem in cloud computing, this could especially be a problem if the vendor closes due to financial issues.

5. Data location: the cloud consumer is not always aware of the location of their data and the cloud provider does not always reveal where the data are kept.

Aamir et al. (2014) say that despite the benefits of the cloud, the largest threat is breaches of security which include, among others, account or service hijacking, data manipulation and data management security. Security is an issue that can be considered from a number of different angles in the cloud, according to Alam et al. (2013) it can include consideration of user access, regulatory compliance, data location, data segregation, investigative support, recovery and long term viability. Y (2013) brings attention to a number of security issues that exist in the cloud which include consideration of privacy, security, compensation for loss of data and liability.

Bamiah et al. (2012) also say that despite the benefits of cloud computing there is a dark side in relation to security and privacy, and this has been the reason why certain industries such as banking and health care have been reluctant to trust the cloud especially in relation to sensitive data. Specifically, the problem is that sensitive data is placed in the cloud with no knowledge of location and there is a lack of transparency about the mechanisms that the cloud service provider uses for securing data and applications (Bamiah et al., 2012). Liang (2012) says that there is a need for better and more comprehensive cooperation between technology vendors and world governments to create unified global rules for a safer government cloud.

A characteristic of the cloud that is a concern for security is multi-tenancy because it virtualises the boundaries between hosted services of the different tenants and therefore, there is a need to strengthen the boundaries with security controls (Almorsy, 2011). The cloud providers themselves have problems related to the cloud platform because it is very complex and there are numerous security considerations (Almorsy 2011). Specifically, these issues include the complex architecture of the cloud platform, it characteristics, the long security stack and the different security needs of stakeholders all of which mean that security has to be continually managed (Almorsy 2011). Moreover, the cloud providers are not aware of the contents of the cloud or the security requirements for the services.

2.3.3 Sensitive and Non-Sensitive Data

E-government data is sensitive data and needs to have a corresponding security mechanism (Bo, 2013). Cloud services are evolving with an increase in the use of cloud technology,

which means that increasingly sensitive data is geographically dispersed in remote servers and locations with the possibility of being exposed to malicious behaviour (Ahmed and Hossain, 2014). Alshomrani and Qamar (2013) say that when third parties store sensitive data, then there are likely to be trust issues for government.

Security and privacy considerations do have implications for managing private and sensitive data, therefore, for governments one of the main decisions that have to be made is whether or not to host sensitive and private data in the cloud (Yamin, 2013). Specifically, sensitive government data could include security, defence and personnel data (Yamin, 2013).

Due to the aforementioned security concerns, a major issue about the adoption of the public cloud is what type of data, whether sensitive or non-sensitive, can be stored in the cloud. Bhatt (2012) says that sensitive data should be kept in corporate (private) clouds and non-sensitive data can reside in public clouds and Khan et al. (2011) say that a private cloud should be established which is operated by government for critical and sensitive government information. Similarly, during analysis of the benefits of cloud computing for e-government in general, and the benefits that it can have to help developing countries to leapfrog, Khan et al., (2011) suggest that critical and sensitive government information be stored in a government private cloud and for general services where government has less control over their provision, the public cloud solution is recommended. This idea has been echoed by Bhatt (2012) who says that sensitive data should be kept in corporate data centres and other data can be kept in the public cloud. Moreover, Lecklider (2014) says that for government agencies in the US, such as the Department of Defense, that there are some data that is too sensitive and will never be put in a commercial cloud. This issue is also a concern for Diez and Silva (2013) who say that there needs to be careful consideration about what services can be migrated to the cloud, and there are certain services that cannot be migrated. Diez and Silva (2013) notes that personally identifiable information is at risk, especially in the public cloud, a suggestion is to anonymise the data before moving to the cloud.

Diez and Silva (2013) say that sensitive data should be processed, stored and communicated using the same protective measures that are used for internal systems in addition to the specific measures that are required for cloud services, this includes authentication, authorization and compartmentalization which is to limit access on a need to know basis. Importantly, governments should consider authentication and identity management as crucial

because sensitive data is stored in cloud servers in addition to the client's servers (Ahmed and Hossain, 2014).

Ahmed and Hossain (2014) say that there are sensitive states or scenarios that are a concern in cloud computing and they include the transmission of personal sensitive data to the server in the cloud and the storage of client's personal data in servers that are remote and not in control of the clients.

2.3.4 Legal and Regulatory Compliance

Governments are bound by laws that govern the protection of data, especially sensitive data related to its citizens. Problems arise in cloud computing because the servers can be located in different geographical jurisdictions which have their own data protection laws. This leads to issues with the governance of the data, an example of which is where governments could subpoena the data of other governments.

Hana (2013) says that an important concern for government in the cloud is achieving compliance with national and international regulatory and legal frameworks. Diez and Silva (2013) says that compliance requirements in public organisations are more difficult to achieve in the cloud environment for reasons that include access to log files and auditing information.

Bhatt (2012) brings attention to the fact that the benefits of cloud computing can be undermined if political and geographic borders become fractured. Diez and Silva (2013) says that legal issues related to data protection are the most important in the area of cloud computing and therefore, before planning any technical details for implementation it is important to consider the legal requirements, this is especially the case in the EU where public organisations are not allowed to send data out of the EU, due to the EU Data Protection Directive (Hashemi, 2013) and the US where the Patriot Act allows the government to seize data for investigation purposes.

Compliance is an issue that has to be considered in the SLA agreement between the client and the service provider. It is important for the client to be aware of the potential legal implications of transferring data from one country to another, considerations include the requirement of meeting specific standards, for example, where personal data is transferred outside of the EC then it should comply with the EC Directive on Data Protection where the adequacy of third country to protect data should be assessed (Australian Government, 2011).

It has been claimed by Hon et al. (2012) that the role of service providers regarding the compliance obligations of their clients is not well defined or understood by the service providers. There is the that during consideration and negation of terms, which are often standard, there was little consideration by the cloud provider of the legal and regulatory obligations of the user and that the user had compliance responsibilities to regulators, this is especially the case in Europe (Hon et al., 2012). Importantly, in the study by Hon et al. (2012) large global service providers have not conducted a legal and regulatory review of their services and terms of service. Despite the fact that some providers have shown that they often refuse to negotiate security and privacy terms, if clients refuse to sign the agreement, then the provider would then agree to make some changes (Hon et al., 2012).

Users of the cloud are not particularly concerned with the issue of colocation of data within a third-party data centre, but rather they are concerned with the geographical location of their data centres, therefore, it is recommended that providers have to reveal to the clients the location of the data (Hon et al., 2012). Haag et al. (2014) say that within public organisations there is uncertainty when it comes to jurisdiction and compliance at a global level because the nature of cloud services being cross-border and distributed which instill in governments an attitude of wait and see.

Technically, it is difficult to verify that data is processed where it is claimed by the provider and often providers can be misleading (Hon et al., 2012). However, although there may be uncertainty about data being outside of Europe, providers often provide assurance that data will not be located in the United States due to the Patriot Act. Diez and Silva (2013) brings attention to the fact that the Federal Information Security Act (2002) in the United States requires that sensitive data must remain within the country, and this is something that cloud service providers have to comply with in order to be certified for government services in the US.

In consideration of the above issues, governance, compliance and security and privacy, and the need for companies to have a certain level of knowledge and control over systems and data, these considerations are in addition to the effectiveness, efficiency and cost consideration for adopting cloud technology (Huntgeburth, 2015).

2.4 Disaster Recovery Continuity in the Cloud

Disaster recovery and business continuity are naturally a critical consideration for clients of the cloud in service agreements. Threats to business continuity can include interruption to communication networks, software or hardware failure, power failure and finally, disaster which result in a loss of access to the service (Australian Government, 2011). Craig et al. (2009) say that business continuity is a challenge in the cloud and this can be addressed by effective remedies which include strong contracts and effective SLAs which stipulate disaster recovery and business continuity plans. Nycz and Polkowski (2015) say a concern of cloud computing is to ensure continuity of access to data even in the event of server failure. In 2011, the Cloud Security Alliance provided security guidance for critical areas of focus in cloud computing and one of those critical areas was disaster recovery, where an important aspect of cloud storage is how it can be used for disaster recovery. The challenges in this area include mobility, information transfer both to and from the cloud and availability (CSA 2011).

Hashemi (2013) says that the use of cloud computing is important to replicate copies of both data and systems in multiple locations. The Scottish government, in their 2014 strategy for a digital future using data hosting and a data centre, address the need to have greater continuity and disaster recovery capabilities for new and existing systems which will require additional hardware and software and the strategy says that cloud computing should be the first consideration for this continuity and disaster recovery strategy (Scotland, 2014).

Decman and Vintar (2013) looked at the literature related to digital preservation and investigated a framework for digital preservation in the public sector and then linked this with cloud computing. The idea behind their suggestion was the long term digital preservation of data for the public sector, the solution was a centralized repository using cloud computing, specifically, a community cloud. The findings of their study included the mapping of six factors of digital preservation to three levels of digital preservation shows that using appropriate steps supported by suitable strategies and policies enables the public administration sector to take advantage of modern information technology and solve the demanding and critical problem of digital preservation (Decman and Vintar, 2013).

The use of the cloud for disaster recovery is something that is also considered by smaller local government, although it is important to note that while there are advantages of using the

cloud for local government because it is easier and more cost effective, they are not jumping into the technology straight away and are being cautious due to security concerns (Barkin, 2013).

2.4.1 Estonia / Microsoft Project

Cloud technology and the way it is used by governments are continuously developing and the latest development is the use of the cloud for virtual data embassy. The Estonia / Microsoft project was started in September 2014 and continued into 2015. The government of Estonia has embarked on a project to open its borders to e-residents who can sign up for digital identification cards which will allow them to access national electronic services and databases (Anthes, 2015). This is part of an overall move of government services into e-government by the government of Estonia which requires the transfer of many databases and services to the cloud, specifically the public cloud. However, there are associated security risks, in 2007 there were a number of denial of service attacks that Estonia blamed on Russia which lead to national concerns about data integrity and data protection (Anthes, 2015). This attack together with the perception of a threat of more attacks, especially in the form of a physical incursion, prompted to decision to move e-government services to the cloud.

Often governments when using cloud solutions for e-government will use private clouds whereby the cloud infrastructure is physically located within their borders or within their embassies in other countries. In terms of security this offers benefits because they can implement their own firewalls and the IT departments have direct control over the data. This security is particularly important because governments need sensitive data and mission critical systems, as well as non-sensitive data, to be in the cloud, especially for back up and disaster recovery purposes. Where governments do use public clouds, the benefits of which include cost, there are security issues and often only non-sensitive data and non-critical systems are put in the cloud.

However, in the case where a country wants to ensure that there is digital continuity where their physical infrastructure, which supports their private cloud, is compromised then they need to look at a public cloud solution whereby data and systems are stored in multiple virtual locations around the world. This will ensure that a government can continue to function in the cloud and provide e-government services to its citizens even in the event that their physical infrastructure and sovereign territory is compromised. This can be achieved on an indefinite basis using virtual embassies. Although the use of embassies as data centres, or

'physical data embassies' is not new, there is a newer idea of virtual data embassies in the cloud as opposed to physical data embassies, whereby data and applications are hosted in the public cloud (See figure 2.1).

Figure 2-1: Estonia's Advanced Digital Continuity (Elements of the Data Embassy Initiative)

Source: Ministry of Economic Affairs and Communications and Microsoft (2015)

This is a very new idea and Estonia is a country that is looking at this solution. Estonia is worried about a threat to its territory from Russia as well as cyber warfare and is working with Microsoft to provide such a 'virtual data embassy' solution where all of its e-government systems will be virtualized. However, because of the security concerns of using a public cloud solution, Estonia is only trusting Microsoft with non-sensitive data to begin with, in this case the President's home page and the government Gazette, before incrementally introducing more sensitive data over time as trust and security are established. The goal is for the Estonian government to achieve complete virtualisation of its e-government systems (Ministry of Economic Affairs and Communications and Microsoft, 2015).

Currently the government of Estonia uses a Physical Data Embassy Solution whereby they have their own physical servers in Estonian embassies around the world and use data centres

in friendly countries. This solution is essentially a private cloud that is geographically distributed. One of the key features of this approach is that the government is in full control of the servers and data security. However, the intention of the Estonian government is to use geographically distributed public clouds, a virtual data embassy solution (Ministry of Economic Affairs and Communications and Microsoft, 2015).

It is important to note that the intention of the Estonia government is not to use the cloud for normal back up and disaster recovery, they see it as a more permanent solution. The main reason for this is that Estonia is in fear of a physical incursion by the Russians into Estonian territory or a cyber-attack on its IT infrastructure, even its private servers located in Estonian embassies of friendly countries. In this case, there would be a need for a solution where all systems and data are functioning in the cloud so that the government can continue to provide online services on an indefinite basis, because in this situation they will not know when they can return to using normal infrastructure.

Although a government using the public cloud is not something unknown, it is still a relatively new idea and only non-sensitive data and non-critical systems are, if anything, considered due to security concerns about the public cloud, and even then, it is for normal back up and disaster recovery purposes (Ministry of Economic Affairs and Communications and Microsoft, 2015).

Until now the Estonian government has only been testing the idea of a Virtual Data Embassy Solution (VDES) using PCC with non-sensitive data as a Beta test with Microsoft using Azure, this is because of the security concerns associated with the public cloud. The ultimate intention is the deployment of more sensitive data and critical systems.

Advanced continuity is the new area or next step for governments using the cloud to provide their services. Cloud technology and the way it is used by governments are developing all the time and the latest development is the use of the cloud for a virtual data embassy solution. The Estonia / Microsoft project was started in September 2014 and continued into 2015. This brings new security considerations using this approach.

2.5 Models of Adopting Cloud Computing in the E-Government Context

Research investigating the use of cloud computing for e-government has been carried out since 2009. There are two significant approaches within the literature to this subject. Some researchers focus on the benefits and challenges of cloud computing for e-government (ATSE, 2010; Bhardwaj, Jain, & Jain, 2010; Chandrasekaran & Kapoor, 2011; Craig, et al., 2009; Das, Patnaik, & Misro, 2011; Kurdi, Taleb-Bendiab; Liang, 2012; Mukherjee & Sahoo, 2012; NASR, et al., 2012; Paquette, Jaeger, & Wilson, 2010; Randles, & Taylor, 2011; Rastogi, 2010; Sharma & Thapliyal, 2011; Tripathi & Parihar, 2011) and other researchers provide models for migrating e-government services to the cloud (Ahmad & Hasibuan, 2012; Chandra & Bhadoria, 2012; Chanchary & Islam, 2011; Das, et al., 2011; Khan, Zhang, Khan, & Chen, 2011; Kurdi, et al., 2011; Liang, 2012; Mukherjee & Sahoo, 2012; NASR, et al., 2012; Rastogi, 2010; Prasad, Chaurasia, Singh, & Gour, 2010).

2.5.1 Challenges and Benefits of Cloud Adoption

Mohammed and Ibrahim (2015) review and classify the models for the adoption of cloud computing by e-government. The main criticism by Mohammed and Ibrahim (2015) was that most of the literature related to cloud computing and e-government is concerned with the benefits and challenges and that there are few studies that are concerned with models or frameworks for adopting cloud computing for e-government.

Rastogi (2010) identified the current problems with e-government architecture and then proposed a model to implement cloud computing into e-government. The model consists of continuous improvement from traditional computing to cloud computing, comprising of four steps which include learning, organisational assessment, cloud prototype, cloud assessment and cloud rollout strategy. While the proposed model offered considers both the organisational issues and the cloud issues, there is very little mention or consideration of relationship factors towards achieving the desired cloud goals of government. There are two phases of the model where negotiation with the CSP (cloud service provider) would be taking place and they include the cloud assessment stage where there is no mention of relationship factors with the CSP and the cloud roll out strategy where only communication with internal and external stakeholders is mentioned.

Liang (2012) looked at the benefits of cloud computing in terms of how it could answer some of the limitations of e-government and proposed an architecture, deployment and service model selection strategies. For the architecture, there are five layers the infrastructure layer which comprises the physical resources and kernel software, the application platform layer, the application layer, the management layer and the client layer. As for the deployment model, Liang (2012) made a comparison, related to cost and security, between the four cloud models, namely; private cloud, community cloud, public cloud and hybrid cloud by identifying the target departments for each of the models, additionally, the characteristics of the service layers (IaaS, SaaS and PaaS) and the associated target businesses were identified. While Liang (2012) does bring attention to the important considerations for government in selecting the type of cloud and the service model approach to support e-government services, there is no mention of any of the relationship aspects with the CSP where all requirements would be achieved. The cloud related critical success factors for success in the cloud are given much attention and they include security and privacy, reliability and sustainability and adherence to legal requirements by the vendor but there is no mention of how these are achieved through the relationship.

Das et al., (2011) talk about the adoption of cloud computing for e-government in terms of reducing costs and increasing scalability and security, in addition to accelerated implementation.

2.5.2 Practical Frameworks

Kurdi et al., (2011) developed a framework with guidelines and tools to support the readiness of e-government information systems in relation to moving to the cloud. The framework provides a method of assessment for readiness for moving to the cloud and is comprised of four dimensions; technological, organisational, people and environmental. The technological aspect includes the ICT infrastructure; the organisational aspect considers organisational size, structure, culture, vision and strategy, leadership, support, legislation and data sharing, the people and stakeholder's aspect includes business, government and citizens and finally, the environment and society block which includes the country profile and demographics, the political, the socio-cultural and the economic considerations. The output from all of these aspects helps governments to understand the important issues related to implementation of e-government systems as well how to assess readiness for migration to the cloud. While this appears to be a comprehensive approach to cloud adoption because it considers the technical,

the organizational, people and environmental, all relevant parties within these areas do not include the CSP, there is particular attention paid to stakeholders in their study but these are citizens, government and business and do not include those who provide the cloud service as a solution for e-government.

Mukherjee and Sahoo (2012) proposed a framework that can be used by all and comprises of three layers, the knowledge base layer which contains the rules and facts about a specific problem from which the system gains expertise, the inference engine layer that scans facts and rules in order to provide answers to users' queries, and finally, the user interface layer which comprises of the channels through which the user communicates with the system.

Ahmad and Hasibaun (2012) propose an architecture comprising of six layers, namely; infrastructure, virtualisation, management, user, access, service and layers. The architecture allows better sharing of information and resources and promotes standardisation in government resources; however, the writers recommended the hybrid cloud model for this deployment.

Chanchary and Islam (2011), in relation to e-government in Saudi Arabia, present a model where systems and critical data are outsourced to the public cloud while at the same time maintaining control centrally.

Singh (2012) proposed a model for transferring e-governance from traditional computing to the cloud using a step by step approach for migration of e-government to the cloud and is comprised of six steps; learning, requirement specifications, cloud prototype development, data and application migration, cloud rollout, and finally, cloud advancement and is a continuous improvement process. Again, although attention is brought to the issues that government face, there is no mention of the relationship with the CSP and how these issues can be resolved.

Song, Shin and Kim (2013) propose a framework to deploy e-government in the cloud which includes three phases, namely; policy, technology and service introduction system. Specifically, it aims to develop the introduction system by considering both technology and policy. Although there are recommendations to tackle government-specific concerns associated with use of the cloud including guidelines on achieving governance, such recommendations are for the internal parties of the government such as departments and ministries, and there is no mention of external parties.

Wang and Hua (2011) proposed a model that considers the user group, the organizer (comprising of the internet service provider and the cloud provider), and the participator (including the application and content supplier, solution supplier, hardware and software, terminal provider and advertisement agent).

Trivedi (2013) presents a model for adoption of cloud computing by government, the framework assists governments to understand the capabilities they need to acquire in order to be able to adopt cloud computing. The TOE framework identifies the technological, organizational and environmental factors in adoption of the cloud.

Mohammed and Ibrahim (2015) classify models into four main types which are layered based, step based, component based and conceptual / theoretical models. Layered based models are either built using the cloud computing architecture service model or by using the traditional e-government architecture and introducing cloud computing in some way. The main focus of these models is how e-government can take advantage of the benefits of cloud computing, however, these models do not pay attention to the challenges (Mohammed and Ibrahim, 2015). Step based models are focused on integrating the current e-government system with cloud computing or simply migrating e-government to the cloud. These models are only concerned with the process of migrating existing systems to the cloud by using a model based on the prototype model of the software engineering. Component-based models are static models which integrate the components of e-government with cloud computing in order to show the benefits of cloud computing. Conceptual or theoretical models look for the factors that influence the adoption of cloud computing by e-government.

Mohammed and Ibrahim (2015) provide a statistical analysis of all the different types of model found in the literature and found that most proposed type of model was the component based models at 42 %, followed by layered based models at 29 %. The least proposed model type was the conceptual / theoretical based models at only 12 %.

2.6 The Government and the Cloud in Saudi Arabia

Cloud services is something that is not widely adopted in Saudi Arabia and there are a number of reasons cited for this. Mreea and Munasinghe (2016) towards understanding why public organisations in Saudi Arabia are reluctant to adopt the public cloud look at the

business, financial and technical attributes of public organisation in order to provide a balanced view of the situation.

The acceptance of the cloud in Saudi Arabia has been addressed by Alharbi (2012) using the Technology Acceptance Model. The study focused on the users' perspectives but was restricted to the TAM model because it also included personal factors such as gender, age and job domain, overall the study found that there was a high level of acceptance by users.

There has been one study, Sharma et al. (2016) that has looked at cloud adoption by public organisations in Oman, however, it focuses on employees of these organisations using the Technology Acceptance Model (TAM). The study goes further to say that there is a need for further research for Gulf countries, which includes Saudi Arabia, to test the human-related factors which includes job opportunity and system-related factors which includes perceived usefulness, perceived ease of use and trust.

Yamin (2013) says that an important part of government reform is to make government more accessible to business, however, this is not possible unless there is government initiative in countries such as Saudi Arabia. Moreover, there are many private business organisations in Saudi Arabia who would benefit greatly from the government being in the cloud. It has been found that number of large organisations in Saudi Arabia such as the biggest mobile phone operator and the utility companies are fully aware of the benefits, this has included the energy sector of the government where there has been a reasonable awareness of the benefits of the cloud (Yamin, 2013). In Yamin's (2013) study there were reasons given for the Saudi Arabian government's reluctance to adopt the cloud which included concerns about security and privacy.

A more recent report in 2016 (Saudi Tech Report, 2016) showed that there has been a very slow uptake of the cloud in Saudi Arabia, and one of the reasons has been the downturn in oil prices which has affected government spending. However, it has been suggested that adoption of the cloud by the Saudi Arabian government would help to drive economic development (Saudi Tech Report, 2016).

There are number of economic initiatives in Saudi Arabia which require using cloud solutions. This includes the construction of smart cities which very much dependent on IT-based systems especially cloud computing (Saudi Tech Report, 2016).

However, there is a negative side to the deployment to the cloud for the Saudi government and that is the cyber security generally in the Middle East. Saudi Arabia is in a particularly vulnerable position in terms of cyber-attacks (Saudi Tech Report, 2016). However, most of the interest and the growth of the adoption of the cloud is clearly taking place in the private sector in Saudi Arabia.

Despite there being interest for use of the public cloud for higher education institutions in the country, there is still recognition that it means that data will be stored outside of the country which could entail data privacy and legal risks (Tashkandi and Al Jabri, 2015).

There is evidence that the government itself is not an influencing factor for adoption of the cloud in Saudi Arabia. According to Tashkandi and Al Jabri (2015) institutes of higher education both private and public say that the government do not play any influencing role in the adoption of the cloud. However, according to Alkhater et al. (2014) the environmental context has a significant influence on cloud adoption in Saudi Arabia, and it is government regulation that defines this context.

Saudi Arabia is a developing country, and according to Sharma et al. (2016) in reference to the motivators of cloud adoption in developing countries, governments face hurdles which include a lack of in-house expertise, trust issues with the technology, the lack of a regulatory authority and the overall lack of will.

It would be important in a study that addresses the relationship reasons and reasons associated with cloud factors that are affecting cloud adoption by the government of Saudi Arabia, to comment on the Saudi government cloud computing initiative. The initiative recommends that cloud computing should be self-provisioned (Ministry of Communications and Information Technology, 2017) which suggests a private cloud solution. In fact, the initiative mentions the current status which only includes Government Secure Network (as IaaS) and Government Service Bus and National contact Centre (as PaaS) and e-correspondence (as SaaS).

Recently in 2016 the Saudi Arabian government have put forward proposals for regulating the cloud in the country. Specifically, this regulation was proposed by the Communications and Information Technology Commission (CITC). The CITC by law is authorized to regulate the information and communication technology in the country and in 2016 review existing

regulations for cloud computing. The CITC say that there is a need for regulation because there has been an increasing demand for the cloud from both the private and public sectors.

The Saudi regulations include a provision that says the following: '*CSPs may not provide, or allow another party to provide, to any third party (including, but not limited to, any individuals, legal entities, domestic or foreign government or public authorities) User Content or User Data belonging to a Cloud User, or process or use them*' (Communications and Information Technology Commission, 2016 s.3.4.2, p.32). Therefore, there is evidence of strict stipulations for government use of the cloud in Saudi Arabia. Furthermore, there is evidence in the regulations that reflect the concerns that government have about loss of governance in the cloud, specifically, the regulations stipulate the following: *CSPs shall grant Cloud Users the right and the technical possibility to access, verify or delete their User Data* (Communications and Information Technology Commission, 2016 s 3.4.3, p.33).

In reference to contractual obligations a number of sections in the regulations clearly stipulate the duties of the CSP which include proof of the CSP's authorisation to use other CSP's for data centres and infrastructures (s 3.6.2). This point has reference to the issue of third parties in the cloud which is a well-known concern for all governments. The regulations also stipulate what CSPs are required to include in the contract which include rules for handling user content which also includes processing, destruction and restoration of data, and the SLA.

2.7 Risk and Trust

Towards understanding the relationship reasons for reluctance of government to adopt the public cloud, which include issues of trust and risk in the cloud and the CSP it is necessary to understand relevant theories of risk and trust in relationships.

2.7.1 Theories of Risk and Trust

Protection Motivation Theory (PMT) is a common theory that is related to risk perception and risk tolerance. The theory says that people will protect themselves when they perceive a risk; they try to avoid negative consequences and feel that they have the ability to carry out preventative measures. Basically, the theory suggests that there is a relationship between risk perception and injury and that an organisation will take action if they are motivated and have the means (Campbell Institute, 2014), however, if they do not have the means, i.e. governance, then there will be higher risk perception.

Goo and Huang (2008) bring attention to the trust-commitment theory that is relevant to an IT outsourcing relationship. The theory basically suggests that trust and commitment are both central to the success of this type of relationship, and there cannot be one without the other. The theory considers the benefits of a relationship, the cost of breaking a relationship, shared values, cooperation and uncertainty in the relationship (Goo and Huang, 2008).

Another theory that may provide an explanation about why governments are reluctant to place sensitive data in the public cloud is risk Compensation / Risk Homeostasis Theory. This theory basically states that a person will take more risk when there is greater security; risk taking behavior is directly related to the safety measures that are in place (Campbell Institute, 2014).

Service procurement, especially at the public level and especially in public cloud procurement where, for example, citizen data is concerned involves complex risks because the procurement process itself is complex. In the literature about collaboration and partnership it can be found that there is a link between relationship risk and trust.

Firdous (2011) says that there no single agreement on the definition of trust, however, there are key factors that are common and they include that trust is important when the environment is uncertain, decisions are made based on trust, trust is based on prior knowledge and experience, trust is subjective, trust changes over time, trust is dependent on the context and finally, trust is multi-faceted. Alruwaili and Gulliver (2014) adopt the idea of reliability trust and they say that trust is subjective and is based on the idea that an individual will perform an action that will affect the welfare of another.

2.7.2 Trust and Relationship

In reference to collaboration fluency there has been increasing research about collaboration and partnership in public sector procurement and has been addressed from different viewpoints including efficiency, effectiveness, performance and success. Unfortunately, however, Grudinschi et al. (2014) say that there have been few studies that focus on procurement in the public sector.

Collaboration efficiency refers to the cost of collaboration which is not directly related to the aims and objectives of the present study. Collaboration effectiveness is about evaluating the ways that objectives are achieved from a managerial perspective (Grudinschi et al. 2014).

Finally, there is concept of collaboration success which is related to satisfaction or dyadic sales (Grudinschi et al. 2014).

Collaboration is essential to achieve high quality services and even though collaboration practices and relationships have been evolving, the achievement of fluent collaboration between the partners is still difficult (Grudinschi et al. 2014). Collaboration fluency is a newly defined concept and is considered to be similar to collaboration effectiveness, and it takes into account managerial indicators such as identifying common goals and challenges. The common goal of the cloud service provider and the government as a customer would include security, planning to achieve the goal, implementing the plan and then analyzing and developing the activity (Grudinschi et al. 2014). Partnerships, in the case of the present study the partnership between the buyer and supplier, are related to the management of collaboration (Grudinschi et al. 2014).

An effective system for ensuring collaboration requires clarity of roles and responsibilities, mechanisms to measure each other's activities especially in terms of roles and responsibilities, and communication in order to enhance the coordination, however, these can be difficult when the communication is relational and not routinised (Thomson et al. 2009).

Norms is based on the idea of reciprocity, that in collaboration each party has a reciprocal obligation to each other and they expect that their contribution will be reciprocated by the partner (Thomson et al. 2009). In the case of the present study, because the government will pay the provider there will be the expectation that the cloud provider will reciprocate by providing the services with the level of security that their government require. Clearly this idea is based on trust which is important in collaboration; unfortunately, this trust takes time and has to be built on a number of different interactions in order to build reputations (Thomson et al. 2009).

2.8 Trust and Risk Perception in the Cloud

As with trust and risk theories generally, trust and risk perception in the cloud are relevant to understand the reluctance of government to adopt the public cloud.

2.8.1 Trust in the Cloud

Trust in the cloud service provider and the services that they offer and the risks that are perceived are major factors that influence the adoption of the public cloud. In this section, the relevant literature towards understanding trust and risk perception in the cloud is presented.

Fan et al. (2014) in reference to existing literature on trust theory, say that trust is considered a measure of uncertainty, the measure of which is represented by entropy. Trust and distrust become significant when consumers are making decisions in an uncertain environment that involves risk and vulnerability. Therefore, Fan et al. (2014) say that cloud service trustworthiness is a function of cloud uncertainty, and it is used in consideration of whether to use the cloud, and the greater the uncertainty of a cloud service system, the lower the trustworthiness (Fan et al., 2014).

Ahmed and Hossain (2014) say that establishing trust is key to establishing a successful cloud computing environment. Moreover, trust in the cloud is something that depends on a number of factors which include automation management, processes and policies as well as human factors and trust is recognised as a soft factor affected by security which is an influencing factor for adoption of the cloud (Ahmed and Hossain, 2014).

Huang and Nicol (2013) raise an important issue in relation to trust in the cloud, they question what exactly the meaning of trust in the cloud is. They question that if the attributes of a cloud service provider are used by the customer as a way to measure trust; on what basis, should they believe the cloud provider and who is the authority who can assess and validate cloud attributes? Here there is clear link between trust and reputation as relationship factors in the cloud that are required to achieve the desired cloud factors. Huang and Nicol (2013) look at the existing mechanisms for establishing trust and also look at their limitations, as solution they offer a mechanism for establishing trust.

McKnight and Chervany (2001) say that there are 16 characteristics of trust organised within five groups which include competence, predictability, benevolence, integrity and other, the latter ‘other’ includes being open, being safe and having a shared understanding.

Abbadi and Alawneh (2012) say that critical infrastructure services and organisations will not place their critical applications in the public cloud without being assured of trustworthiness of the different elements of the cloud without having to understand all of the details about infrastructure. Similarly, Gholami and Arani (2015) acknowledge that there is concern about

place sensitive data in the cloud and say that trust is the solution to enhance security and is an important way to improve reliability.

Filali and Yagoubi (2015) bring attention to the fact that the benefits of the cloud which include sharing services in a dynamic environment, storing data remotely the ability to scale up, can be seen as weaknesses in reference to assuring trust and therefore, instill a lack of confidence.

Ryan and Falvey (2012) say that the perception of trust in cloud computing which is based on centralized servers is often formed by people based on the use of their own computers which are localized in nature. The idea is that this view of trust is based more on perception than fact and Ryan and Falvey (2012) recommended that users of the cloud change their view of trust like has happened with other contexts such as travel and banking.

Wu et al., (2013) say that trust is good way of achieving security and also allows access control, reliability and policies. Similarly, Bhatt (2012) says that cloud customers need to be able to trust that cloud services are safe, and that the issue of security is essential for the building of trust.

Alshomrani and Qamar (2013 p.17) say that trust is an '*act of firm belief in truth, reliability, faith, confidence, or strength of someone or something. It is a belief in the capabilities and skills of others that you think you can reasonably rely on them to care for your valuable assets'*.

Ahmed and Hossain (2014) say that trust is an issue that gives rise to security concerns because it is directly related to the credibility of the cloud service provider. Similarly, there are a number of different ways that enable trust in an unknown entity which includes direct interaction, reputation, trust recommendation, trust negotiation and propagation, Abbadi and Alawneh (2012) say that a trustworthy environment is established through cloud providers continuously enforcing the cloud requirements of the customer, do not interfere with the customer's application data and hand over control of the data from the cloud provider to the user (Abbadi and Alawneh (2012).

Burda and Teutberg (2014) say that trust is something that can be increased through the satisfaction of the user but also by the provider's reputation. It is important to further understand the issue of reputation as a determinant of trust in a cloud provider. Reputation has been identified as being particularly important in research about cloud provider selection

(Burda and Teutberg, 2014). It is important to note that some companies see the cost of being perceived as untrustworthy as very high, especially for those companies who have achieved a reputation for being trustworthy, and therefore, trustworthiness is considered an asset (Burda and Teutberg, 2014). Based on a definition of provider reputation provided by Doney and Cannon (1997), Burda and Teutberg (2014) say that reputation is based on the extent to which a cloud customer believes that a cloud provider is honest and is genuinely concerned about their customers. Huang and Nicol (2013) also say that trust in the cloud is based the perception of reputation. The issue of reputation is addressed by Parwar et al. (2012) who say that reputation-based trust is a good way of evaluating service providers based on available evidence.

In considering trust in a cloud service provider there is also the issue of familiarity, this is considered a prerequisite of trust and it is about the understanding that a customer has of an organisation based on interactions and experience that they have had (Burda and Teutberg ,2014). More specifically, in relation to cloud service providers, familiarity can relate to how well the customer understands the cloud service provider's infrastructure and procedures (Burda and Teutberg (2014).

Brender and Markov (2013) bring attention to the fact that although there are numerous benefits to the cloud, there are still security risks whom the authors identify as information security, regulatory compliance, location of data, provider lock in, support in investigations and disaster recovery. Brender and Markov (2013) found that there was a high degree of risk awareness. Risk can be found in any context and a traditional formula for risk is that risk = probability x impact and involves comparison where one activity is considered riskier than another (Ryan and Falvey, 2012) and risk management decision processes are strongly affected by concerns about security, data availability, confidentiality, integrity and loss of governance (Elena, 2012).

Elena (2012) say there is lack of understanding of risk perception in cloud computing and examines risk perception using psychometric testing in a questionnaire. The results of their study showed the military organisation was more concerned about documents in the cloud.

One of the contributing factors to risk perception of using the cloud is that cloud providers often offer clients standard terms which are offered on a 'click through' basis to accept terms and do not give opportunity to the client to negotiate (Hon et al., 2012). Reasons that cloud providers have this 'click through' approach to contractual terms, which is reflective of a

standardised offering approach, is because they wish to eliminate the cost of negotiation, legal liabilities and other associated risks, moreover, they do not have in-house legal resources to deal with requests for changes to terms as they arise from the client (Hon et al., 2012). However, this approach by service providers can be a risk for potential users because often users will click through the terms in order so that they can start using the technology without considering the effect of those terms, it has in fact been shown that it is common for employees to accept standard terms in this way and then try to renegotiate the terms later to achieve more acceptable terms (Hon et al., 2012). Just because a service is low cost or free of charge this does not indicate that it is low risk or free of risk (Hon et al., 2012). There may exist regulatory or legal risks, especially with data that is sensitive (Hon et al., 2012). According to Hon et al. (2012) even if contracts are negotiated legal professionals of the clients are often not involved in the negotiation.

2.8.2 Trust models

Burda and Teutberg (2014) present a model that considers user's perception of risk and trust in addition to the antecedents of trust, they found that trust can mitigate uncertainty and actually reduce risk perception, and in reference to the present study, Burda and Teutberg (2014) say that risk perception is one of the main inhibitors of cloud adoption.

Burda and Teutberg's (2014) research model clearly illustrates the interaction between satisfaction, reputation and familiarity, perceived ease of use, perceived usefulness, trust, risk and the intention to use. They present a number of hypotheses in their study which include that perceived usefulness will positively affect the intention to use the cloud, a perceived ease of use will also positively affect the intention to use the cloud, perceived risk will have a negative effect on the intention to use the cloud, trust positively affects intention to use the cloud, trust will negatively affect perceived risk to use the cloud, trust will positively affect perceived usefulness and perceived ease of use will positively affect trust. Moreover, reputation is another aspect of trust in relation to the confidence to adopt cloud services, Burda and Teutberg (2014) say that reputation positively affects trust and that familiarity with a cloud service provider positively affects trust and the perceived ease of use.

Filali and Yagoubi (2015) present a general trust model which is based on the QoS (Quality of Service) and the Certain Trust Model and contributes towards the selection of a cloud provider. Specifically, selection is based on sources which include user feedback, direct trust, user preference and Qos parameters and the model considers two trust attributes which

include trust value and performance value, performance value allows trust to be evaluated, and finally, the model uses consumer preferences (Filali and Yagoubi, 2015). Similarly, Manuel (2015) approaches the issue of trust in the cloud from the perspective of service quality, specifically, Manuel (2015) present a trust model for the cloud that is based on past credentials and present capability of a cloud service provider. They say that trust is calculated based on four parameters which include availability, reliability, turnaround and data integrity.

In response to the fact that assurances about the cloud are insufficient and that clients do not have confidence in cloud providers, Chong et al., (2014) offer a multi-faceted trust management system architecture designed to allow cloud customers to identify trustworthy providers. Similarly, Noor and Sheng (2013) propose a framework for trust management based on credibility based on credible trust feedback which also takes in consideration of malicious feedback from attackers.

According to Huntgeburth (2015) agency problems are common in cloud service relationships (the agency problem here being where the actions of the cloud provider as an agent affect the welfare of the government as the principle) and that this is made worse by the fact that quality of cloud service providers is something that is difficult to evaluate because the behavior of the provider and the technical details are hidden from the user.

Therefore, the relationship between the user and the service provider and the ongoing assessment by the user and the decision whether or not to continue with the provider, is affected by uncertainty of the cloud provider where quality is difficult to assess (Huntgeburth, 2015).

2.9 Cloud Service Level Agreement SLA (Negotiation)

In order to achieve the identified benefits of the cloud it is important for governments to establish guidelines that address the associated concerns through the use of effective SLAs (Khan et al. 2011). In a cloud solution situation, the traditional controls that are available with normal systems can be managed through the SLA.

The SLA should include a number of different areas related to security that are listed in the SLA which include user access, regulatory compliance, data location, data segregation, investigative support, recovery and long-term viability (Alam et al., 2013). However, although this paper is concerned with security in the SLA agreement, the legal agreement

between the cloud service provider and the customer, and there is a detailed consideration of cloud related factors, as with the common criticisms of models and approaches to cloud adoption, there is no mention of the SLA relationship factors required to achieve the cloud factors.

Bochicchio et al. (2011) say that cloud contract management plays an important role in the formation of cloud services contracts and should include a combination of legal, financial operational and technical aspects. Bochicchio et al. (2011) say that for government contracts they are far more complex and contain specific requests. Cloud contract management should include consideration of negotiation and collaboration as relationship factors towards achieving the required cloud factors. Bochicchio et al. (2011) do provide the practical ways in which to manage the relationship which includes strategic communication management, business communication management and operational communication management where there is mention of the importance of the need for communication between peers in the customer and provider organisations, however, the level of detail for relationship factors ends there.

Baset (2012) acknowledge the variation in cloud SLAs and says that SLAs leave detection of violation of the SLA to the customer. In order to make comparisons between the different SLAs that are available, Baset (2012) break down SLAs into their component parts. SLAs can be divided into the service guarantee which relates to a service guarantee time period and includes availability, response time, disaster recovery and fault resolution, the service granularity refers to the scale of the resource on which the service is specified, for example, on a per service or per transaction basis. Although this study does much to highlight the problems that are associated with cloud SLAs there are no practical solutions offered.

Zheng et al. (2014) say that if cloud providers and cloud consumers have different preferences it means that a SLA cannot be achieved unless there is negotiation. A solution that is offered by Zheng et al. (2014) is that there should be a mix of concession and tradeoff strategies which they found that as a negotiation approach achieved higher utility than the concession approach and less failures than the tradeoff approach. This study does much to address how compromise and trade-off can overcome the differing intentions of the two parties, however, there is no mention of how relationship factors such as negotiation have an effect on confidence and the only relationship factor that is mentioned is negotiation.

What is relevant to the present study are some of the findings from Baset's (2012) study. Firstly, the study found that cloud providers do not provide guarantees for compute instances and performance and secondly, the burden of detecting a violation of the SLA is left to the customer and that in some cases the service provider requires that the customer has to inform the provider of the violation within a specified timeframe. What the study found was missing from the SLAs were sufficient assurances of disaster recovery, privacy, auditability and security (Baset, 2012).

Burden (2014) say that contracts for the cloud have been extremely restrictive, however, although it has been the case that a few large providers have dominated the market which has led to inflexible SLAs, however, the market is changing and there are more companies entering the market which will be able to offer more flexible SLAs (Di Modica and Tomarchio, 2014).

Burden (2014) does address the trends that are found in cloud computing SLAs and interestingly does address the issue of risk in the relationship, however, this is the risk perception that the CSP has in that relationship on whether to offer more customisable services. What is also important Burden (2014) is that there is recognition that an increase in negotiation has led to a recent shift towards more customisable offerings. Burden informs the present study about what may be important in a relationship that is perceived to be successful for the government as a customer. For example, Burden (2015) recognises the importance of customer knowledge.

2.9.1 SLA Inclusions

The Australian government offer advice about the legal implications of using the cloud, they bring attention to the fact that providers of the public cloud include clauses that they can change the terms of the agreement at their own discretion and advise government to either delete such rights or to oblige the provider to provide sufficient notice.

In reference to service levels, it is important that level of service meets the service expected by the client, this is especially important if the service is critical and the service levels should measure something that is critical to the client, be easy to measure and there should be an incentive for the provider to meet the service requirements (Australian government, 2011). Key aspects of service include response times to interruption of services, flexibility of service

in terms of scalability of service and finally, business continuity and disaster recovery (Australian Government, 2011).

Moreover, it is important agreements are included in the SLA that ensure disaster recovery requirements are met so that the client does not lose service or suffer from serious service disruptions, this may be achieved through a geographically separate disaster recovery site transition to which can take place seamlessly, continuity in the case of a power failure, make business continuity a strict requirement, that business continuity plans are submitted to and approved by the client, limitations on the provider for suspension of services and finally, regular maintenance (Australian Government, 2011).

Other important aspects of the SLA include terms for ending the arrangement, dispute resolution, the disengagement and transition of services and the changes to terms and conditions by the provider (Australian Government, 2011).

Similarly, the Cloud Standards Customer Council (2013) say that the agreement should include service provision, payment, temporary suspension in service, terms of termination, indemnification against loss or damage, limitation of liability and security and privacy.

The customer themselves also have obligations that will be found in a cloud service agreement. Referred to as Acceptable Use Policies (AUPs) they include terms of use for both the customer and the provider, an example includes that the customer will not put any malware in the cloud (Cloud Standards Customer Council, 2013).

Hon et al. (2012) examine cloud contracts that are negotiated, specifically, they look at the area of where users make requirements to change standard terms and the extent to which the providers agree to such changes. The findings of their study show that the most negotiation takes place in the areas of liability, Service Level Agreement, security and data protection, termination rights, amendments to service and intellectual property rights. Where clients should more seriously scrutinize the terms of an agreement is where there is consideration of full migration to the cloud or where ‘real’ or personal data is considered (Hon et al., 2012). Rajavel and Thangarathinam (2014) address the issue of negotiation conflict which they say arises from misperception, aggressive behavior and uncertainty in terms of preferences and goals.

2.9.2 Dynamic / Flexible SLA

Cloud customer requirements are continuously changing and it is important that cloud services respond, in light of this requirement Prieta et al. (2015) present a real-time agreement and fulfilment of SLAs in cloud computing, the idea is that resources are readjusted to meet change in demand.

Kanwal (2014) say that Active – Passive trust models are considered active if they allow the flexibility to dynamically update the agreement according to changing requirements of cloud customers. These agreements need to be updated periodically because the customers' requirements regarding security and quality of service change over time. These models are considered passive if they're not flexible enough to be updated and manipulated according to the changing requirements of cloud customers.

However, the idea that terms are standardized is supported by Hon et al., (2012) who say that it may be difficult for clients to negotiate terms with large providers who may refuse requests for change because they have more bargaining power, in this case terms may be on a 'take it or leave it' basis. Although there has been the idea that large service providers are inflexible in this sense, there has been move towards by large providers to be more flexible in order to secure contract (Hon et al., 2012).

Negotiation is something that engaged in more by larger organisations, especially those that are regulated and there is demand or insistence that clients' requirements are included (Hon et al., 2012). Although it may be the case that government organisations have the purchasing power and therefore, it seems that they can get what they want, the internal procedures make it difficult to formulate and agree terms (Hon et al., 2012). Larger organisations such as governments demand that the contracts are on their terms and they try to negotiate more.

Going against the argument that cloud contracts are too standardized, Hon et al. (2012) found that there have been a number of different types of approaches to cloud contracts than the standard cloud models, this has been evidenced by participants in the cloud developing a diverse range of cloud services with different contractual terms. Importantly, contracts have been found to consider standards and certifications that promote legal certainty and compliance (Hon et al., 2012).

Although it is the purpose of a cloud provider to offer computing services to clients while making a profit, there are circumstances where the service providers have to differentiate their SLAs because of the type of client (Macias and Guitart 2014).

Rajavel and Thangarathinam (2014) say that there are two types of SLA, those which are classified as static which means they are predefined by the cloud service provider and those classified as negotiated or customized. The former type is often offered by large cloud providers such as Microsoft Azure and Amazon and they are often established as soon as the client has confirmed the consumer service request and made the online payment. Where this template is not appropriate, especially for those consumers that have special QOS requests, Rajavel and Thangarathinam (2014) offer an automated negotiation framework which considers that for the provider there needs to profit maximization while at the same time offering a differentiated SLA according to client types as well as agreement of customised service provisioning.

2.9.3 SLAs and Trust

Alhamad et al., (2010) present a SLA-based trust model for cloud computing and also bring attention to the fact that for critical systems and sensitive data there is a need to select cloud providers based on the requirement for a high level of trustworthiness. The trust model that is presented by Alhamad et al., (2010) is designed to help evaluate cloud services which will help users select the most reliable service. This model was achieved by combining a SLA framework for cloud computing with trust management. Manuel (2015) in proposing a model for trust says that an SLA is based on quality of service requirements and capabilities of the provider.

There are clearly two elements within the SLA-based trust model that is offered by Alhamad et al., (2010), firstly, they talk about the most related services which means services that meet the functional requirements, and secondly, trusted resources.

Alruwaili and Gulliver (2014) say that in addition to confidentiality, integrity and availability concerns, there are also issues of trust especially where the cloud hosts sensitive data. Moreover, Alruwaili and Gulliver (2014) say that the cloud service providers themselves have difficulty in maintaining confidentiality, integrity and availability for their customers.

Alruwaili and Gulliver (2014) highlight the concerns when transferring applications to the cloud, these are three security and privacy concerns and are as follows: cloud service

providers may not possess the required intrusion detection and prevention policies to meet the requirements of the customer, the cloud service provider may not have the necessary intrusion detection and prevention controls which mean that confidentiality and integrity could become compromised whereby customer can lose their data, finally, the cloud service provider may not possess the needed intrusion detection and prevention systems which may lead to a loss of service and a loss of information availability for the customer.

Alruwaili and Gulliver (2014) highlight the trust concerns that customers have when they enter into an agreement with a cloud service provider, and one of the issues that they mention is that customers have insufficient information about their service providers. As a result, it is often the case that customers have to accept a certain level of risk, however, it is important to note that where there is insufficient information about security and privacy services, risks can be mitigated, to a certain extent, by a detailed SLA and a detailed meeting. Alruwaili and Gulliver (2014) say that trust and reputation systems should be combined with SLAs in order to create confidence in the customer.

An important note that is made by Alruwaili and Gulliver (2014) relevant to the present study is that although there have been solutions to address SLA requirements in cloud computing, there is a need to leverage the trust relationship between cloud provider and cloud customer.

Furthermore, one of the requirements that governments would have is that they are allowed to continuously monitor and evaluate the cloud service that they are being provided. Alruwaili and Gulliver (2014) say it is important that there is continual evaluation of intrusion detection and prevention, this brings attention to the idea of continuous evaluation as part of the cloud provider – customer relationship.

Fan and Perros (2014) offer a solution to the issue of trust in the cloud which involves Trust Service Providers which are independent third-party trust agents that are trusted by cloud providers, cloud service providers and cloud customers, these agents are distributed throughout the cloud and that gather raw data about trust related to the extent to which a cloud service providers adhere to the SLA.

A similar idea has been put forward by Pan et al. (2015) which is based on the idea of trust relationships in a social network, which these authors say is something that is not taken into consideration in existing methods of selection of cloud services.

Habib et al. (2012) bring attention to the idea that although most cloud providers offer the same service, the descriptions that are found in SLAs, where technical and functional assurances are specified, are not consistent between the various cloud providers, this means that potential customers are unsure of how to identify a trustworthy cloud provider based on the SLA. Habib et al. (2012) propose a multi-faceted Trust Management (TM) system architecture which helps to identify trustworthy cloud providers based on different attributes which include security, performance and compliance.

Habib et al. (2012) say that there are a multitude of attributes that have to be considered in selecting trustworthy cloud providers. They say that a TM should combine these attributes which are based on user feedback and reviews known as soft trust and certificates or audits known as hard trust.

Marudhadevi et al. (2014) say that during the SLA negotiation customers will have inadequate assurances in order to determine if the services are trustworthy. These authors propose a trust mining model that is used to identify trustworthy service providers during the SLA negotiation. The model is based on objective and subjective ratings, the former from the cloud service provider when their service is used and the latter from the customer when they used the service. Moreover, the model is based on third parties which include a SLA manager who negotiates the SLA between provider and customer and the negotiation is complete when the customer agrees on the trust rate of the provider, and a trust manager who determines trust based on previous and current experience of a cloud providers' customers and then passes that information onto the SLA manager (Marudhadevi et al., 2014). Aamir et al. (2014) identify a number of challenges to security in the cloud and they include weak Service Level Agreements (SLAs).

2.10 Summary

The review of the literature here has provided both an overview of the issues relevant to the present study and overview of similar work that has been carried out in this area. Review of work that has already been done in the area of cloud adoption has showed the research gap of this study. The review has shown that although there is consideration of trust and risk issues and cloud related issues such as security and privacy and governance, they are not considered together.

From the literature in the above it can be seen that much attention is given to issues that relate to the suitability of the cloud and the benefits and risks of the cloud. There has been very little literature written about the relationship between the customer and the CSP in relation to specific areas of the cloud, especially government and the public cloud.

Some studies focus on the human-related factors in cloud adoption as opposed to technology-related factors, such as those that use the TAM, however, there is lack of studies in the literature about the actual relationship and relationship factors between the customer and the cloud service provider. Where risk and trust are addressed they are simply established against cloud factors, for example, there is a perceived risk of losing control over data but this is not explored in detail. Moreover, although it has to be acknowledged that negotiation and collaboration between customer and provider are addressed in the literature, the literature does not associate these relationship factors with specific aspects of the cloud, and negotiation and collaboration generally between government and the CSP receives even less attention.

Even though relationship factors may apparently be addressed, such as trust or the perception of risk, they are often associated with technology and its ability rather than the CSPs ability or willingness to ensure required service. Trust and risk are often considered in relation to trust or a perception of risk for the technology to provide a safe and secure service, rarely is trust and risk viewed as a relationship factor between the customer and the CSP where the CSP can be trusted to provide the required security, or the required security can be negotiated or collaborated for within the relationship. Therefore, as a solution to the problem of reluctance by government to adopt the public cloud, this study considers the relationship rather than the technical.

3 Research Design

Objectives

- **To present the research design of the study**
- **To identify relevant cloud and relationship factors**
- **To demonstrate relevant links between relationship and cloud factors**

3.1 Introduction

Research into information systems (IS) is not purely technical nor is it purely social and is in fact a combination of the two, referred to as a sociotechnical approach (Sarker et al. 2013). This sociotechnical approach tries to understand the interaction between the technical aspects which include technology and the business processes supported by this technology (Huntgeburth, 2015), in the case of the present study this would be the technology that is used not only to offer the cloud services to government but also offer the ability to govern data and processes, be compliant and be secure as a service. The social aspects are the values and the needs of the people in an organisation (Huntgeburth, 2015); again, in the case of the present study the people are the government that are the purchasers of the cloud and the requirements and concerns that they have. These requirements are achieved in the relationship between government and CSP.

According to Huntgeburth (2015) in more recent years IS research has focused more and more on changes that are a result of cloud computing, however, there has been no framework for considering the behavioural changes as a result of the emergence of the cloud.

Primarily, the study is concerned with the relationship factors that affect government adoption of the public cloud and the associated areas of the cloud where these relationship issues occur. Therefore, it is important to understand the aspects of a user – provider relationship that have a bearing on the willingness to adopt the cloud. There are certain theories that can be used to understand this relationship and the associated cloud concerns.

One of the main contributions in this area is the Cloud Service Relationship Theory by Huntgeburth (2015) which explains how uncertainties occur in the user – cloud provider relationship and how they can be mitigated. This theory is based on a number of different theories which explain why different aspects of the relationship may be responsible for reluctance to adopt the cloud. In this chapter, the relevant theory related to the relationship and associated cloud factors in the government – CSP relationship in the context of cloud adoption is presented. These theoretical foundations are used to inform the development of the research design of the study.

The research design is developed to help understand how relationship factors link to cloud factors, for example where a government does not trust the governance structures offered by a cloud provider, and therefore, provides insight into the areas of concerns. Moreover, the

study offers greater insight by considering the specific issues within each cloud factor. This is achieved through the consideration of cloud sub factors, for example, where governance is the cloud factor; control over data would be a cloud sub factor. All factors whether relationship, cloud or cloud sub factors are considered in the study as critical success factors for government confidence in the public cloud. These factors form the basis of the development of the methods which include a questionnaire and a semi-structured interview.

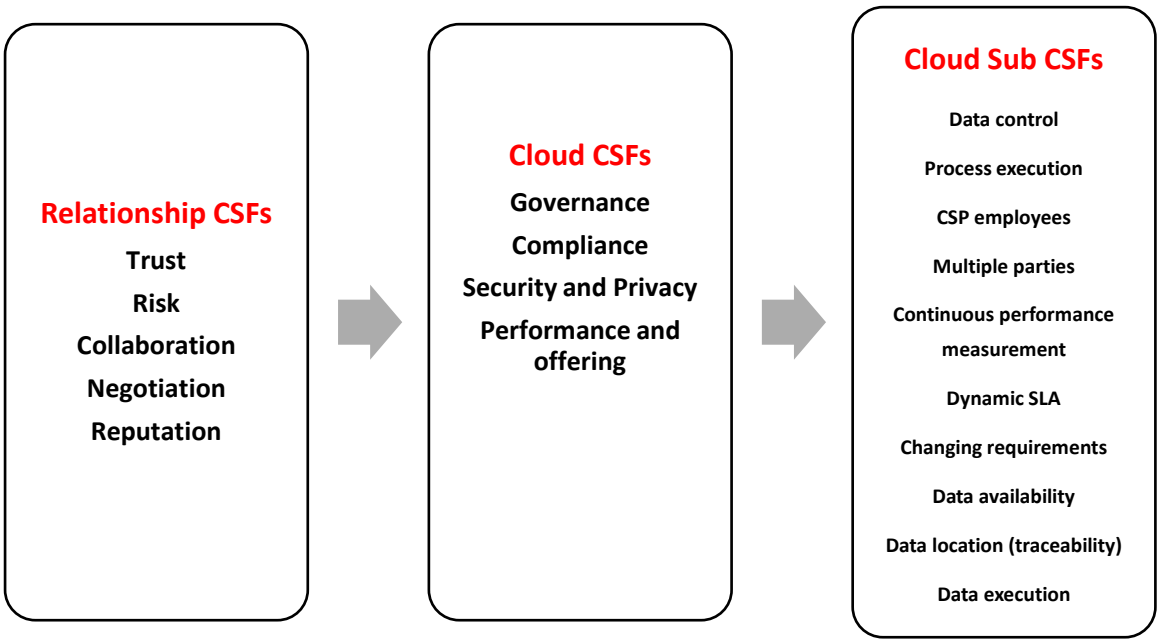
3.2 Research design

The research design answers the research questions and achieves the aims and objectives. The research questions, the first aim and first objective are concerned with the relationship factors that may have an impact on governments' confidence to place sensitive data and critical systems in the public cloud. These factors have been identified from the literature and existing models, frameworks and standards for the cloud. Specifically, the relationship factors are trust, risk, collaboration, negotiation and reputation (Figure 3.1) and are all relevant to the relationship between government and a cloud service provider.

The research questions are related to the cloud factors that are relevant to government when considering the public cloud and the study wants to investigate how these cloud factors are affected by relationship factors, for example, a government may perceive a risk in relation to governance or they feel they are not able to negotiate compliance needs, this is the relationship between relationship factors and cloud factors (Figure 3.1).

Moreover, because the study is about the relationship for the public cloud, greater insight into the specific areas or factors of the cloud is required. An example of this can be seen in the last box in Figure 3.1 where the specific areas within the cloud factor of governance include process execution and cloud service provider (CSP) employees.

Figure 3-1: Research structure - Relationship and cloud factors



3.3 Relationship Critical Success Factors (RCSFs)

Aspects of the relationship that have been shown in the literature to have a direct impact on confidence to adopt the cloud. Specifically, they include trust, risk, collaboration, negotiation and reputation. Although there is often a relationship between these factors, for example a good reputation is required for trust; it is justified to approach them separately because each one receives a significant amount of attention in the literature and have been shown to be relevant when considering the reasons that governments are reluctant to migrate to the public cloud.

These relationship factors, as well as the cloud factors that follow, are considered as critical success factors, for example for there to be a successful relationship and associated confidence to use the public cloud there needs to be increased trust, decreased perception of risk, an effective negotiation and collaborative relationship as well as a perceived positive reputation.

3.3.1 Trust (CSF)

According to Mayer et al (1995 p.726) trust is 'willingness to be vulnerable to another party' and trust is founded in three characteristics which are ability, integrity and benevolence, collectively known as trustworthiness. Moreover, trust is about the users' intention to accept

vulnerability based on the belief that using the cloud will meet their expectations based on the confidence of the cloud provider as well as the cloud integrity and benevolence.

Behavioural attributes of trust include competence, dynamism, expertise, predictability, benevolence, responsiveness, integrity, honesty, credibility, reliability, dependability, carefulness and understanding (McKnight and Chervany, 2001). Additionally, trust is based on expectancy by the customer that the provider would behave in a particular way and belief by the customer that the service provider has integrity, goodwill and competence (Nicol, 2013).

According to Firdhous et al. (2011) trust only plays a role when the environment is perceived to be risky and uncertain, is the basis on which decisions are made, is based on prior knowledge and experience, is a subjective notion based on opinions, can change with time and experience and is dependent on the context.

The latter point about trust being dependent on the context is relevant to the present study where the context is the cloud and the associated cloud factors. In relation to this, the research design of the study is based on the idea that relationship factors such as trust should be considered with cloud factors, this link between the two different types of critical success factor is explained in more detail at the end of this section (Section 3.3.1.2).

3.3.1.1 Trust and IT

Blomqvist et al. (2008) examines the role of trust in contracts in companies that are technology intensive and puts forward propositions about the role of trust and contracting in these types of companies. Trust is about what the other party will do in a situation that is often not included in the contract; in fact, formal contracts only play a limited role and have to be augmented by informal norms and agreements (Blomqvist et al., 2008). Much like the situation in the present study, when companies are engaged in this type of partnership they have to share valuable information and this information cannot always be covered by the contract, therefore, it requires trust. Moreover, similar to ideas put forward by Grudinschi et al. (2014) if the partners are able to trust each other then it will lead to better communication and collaboration, and also enhances the transfer of information. A key consideration here is to what extent are governments allowed to trust cloud service providers given the laws and regulations that they must abide by?

Another point raised by Blomqvist et al. (2008) is that trust is a more important governance mechanism for companies dealing with technology than other companies. Moreover, that instead of being something that takes time to develop trust may be something that can develop quickly if there is an intense interaction of managers negotiating within collaboration and may enable a collaborative relationship (Blomqvist (2002). In fact, as pointed out by Blomqvist (2005) with technology intensive partnerships fast-based trust was essential for partnership formation. Therefore, trust and collaboration are linked, but here it has been shown that trust is something that cannot necessarily be controlled by a contract. In reference to the present study, these ideas can inform the interviews through the development of questions related to trust.

3.3.1.2 Link between Trust and Cloud Critical Success Factors (CCSFs)

Towards achieving the aims and objectives of this study where both relationship and cloud factors are considered together towards understanding government reluctance to adopt the public cloud, and towards the development of research methods to achieve it is necessary to show the link between trust as a relationship factor and cloud factors. Where trust is considered it has to be considered with cloud factors which are impacted by trust and vice versa. Habib et al. (2011) says that trust has been shown to be linked with cloud factors such as security, performance and compliance and trust has been associated with reputation factors where trust is based on feedback and reviews.

In reference to the cloud specifically, Noor et al. (2016) says that poor trust management is one of the main reasons for lack of adoption of the cloud and associates the trust characteristics of the cloud with security and privacy of sensitive data through authentication and authorization. Moreover, the responsibility for this security as a cloud factor should be included in the Service Level Agreement (SLA) which both parties negotiate.

Further links between trust and cloud related factors have been made by Khan and Malluhi (2010) who say that trust in the cloud from the perspective of the user is related to the security and privacy of data. Moreover, in reference to governance, Khan and Malluhi (2010) say that control ownership prevention and a lack of control and transparency decrease trust and that providing more jurisdiction and allowing for remote access control facilities and transparency will increase trust.

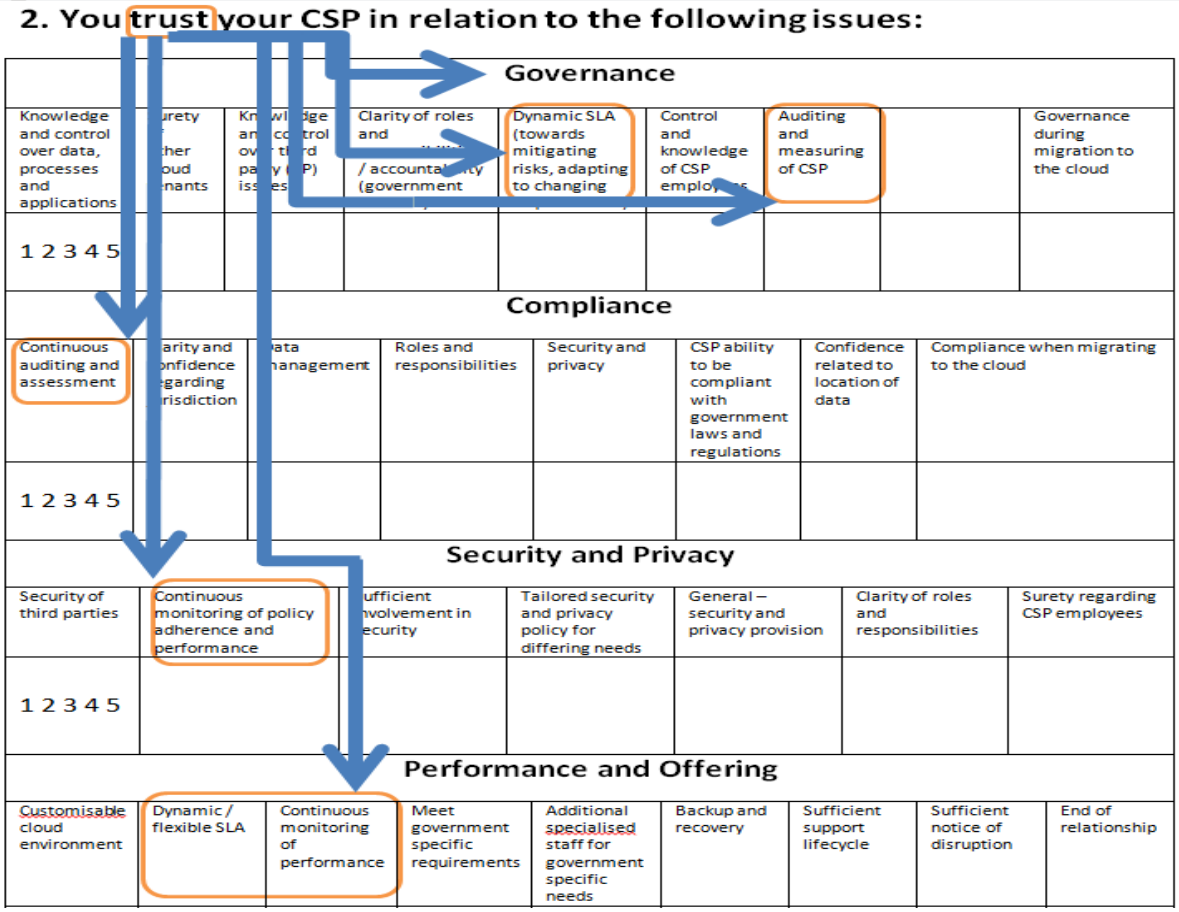
Fan and Peros (2014) say that a trust issue is that multiple clouds can be used by cloud service providers run on distributed computing resources. They say that for a multi-cloud solution a trust relationship is required among customers, cloud service providers and cloud providers. Fan and Peros (2014) also say that trust can be considered objective trustworthiness when based on quality of service (QOS) and subjective trustworthiness where users' perception of belief in a cloud service provider is based on their preferences and requirements.

3.3.1.3 Link between Trust and Sub Cloud factors

In addition to the established relationships between trust as a relationship CSF and the cloud CSF there is also evidence of links between trust and sub critical success factors of the cloud. To provide an illustration, trust as a relationship factor has been shown in the literature (Nycz and Polkowski, 2015, Ahmed and Hossain, 2014, Alshomrani and Qamar, 2013) to be related to governance, compliance, security and privacy and performance and offering as cloud critical success factors, however, each of these has sub critical success factors that also have a relationship with trust, examples include continuous auditing and assessment and dynamic / flexible agreements.

Kanwal (2014) says that in agreement-based trust models it is a functional requirement that there is dynamic update and monitoring of agreements in order to maintain trust, this can be in the form of contract parameters monitoring. Cloud CSFs and their associated sub cloud CSFs are relevant here. In order to achieve governance as a cloud CSF and therefore, trust, the sub cloud factors of a dynamic service level agreement (SLA) and auditing and measuring of the CSP need to be achieved. This is also the case for other cloud CSFs, for example, compliance requires continuous auditing and assessment, and performance and offering also require a dynamic SLA and continuous monitoring of performance (see Figure 3.2).

Figure 3-2: Relationship between Trust and Cloud Sub Factors



Where trust is associated with the cloud it has been shown to be an ongoing trust that is achieved through continuous measurement of performance and dynamic agreements which can change with changing requirements and that these types of trust are to be found in all areas of the cloud, namely; governance, compliance, security and privacy and performance and offering and their associated sub cloud factors such as a dynamic agreement and continuous monitoring of performance. Therefore, trust is a relationship CSF that has an association with the cloud CSFs and the sub cloud CSFs. The idea of these links is found in the literature and it is important to include this link in the research of this study in order to not only understand the role of trust in the relationship, but also to find out which aspects of the cloud where trust has an impact towards understanding government reluctance to adopt the public cloud.

3.3.2 Risk (CSF)

The perception of risk is something that the literature (Abbadi and Alawneh, 2012, Gholami and Arani, 2015, Burda and Teutberg, 2014, Ahmed and Hossain, 2014, Brender and Markov, 2013) has shown to be the main reason that governments do not have the confidence to adopt the public cloud. A reduction in risk perception is considered to be a relationship CSF towards achieving confidence in the public cloud.

Service procurement, especially at the public level and especially in public cloud procurement where, for example, citizen data is concerned, involves complex risks because the procurement process itself is complex. The present study is motivated by the fact that governments do not have the confidence to place sensitive data in the public cloud because they perceive risks. Therefore, it is important to consider the issue of this risk perception within a public procurement relationship. Consideration of how the links between the perception of risk as a relationship factor and cloud factors such as security and privacy is important towards understanding reluctance by government to adopt the public cloud.

In this section the perception of risk is associated with all of the cloud critical success factors, in other words governments perceive a risk in relation to governance, compliance, security and privacy and performance and offering. As part of the development of the research methods the links between risk or the perception of risk as a relationship factor and cloud factors and sub cloud factors is presented here.

3.3.2.1 General Theories and Ideas about Risk

There have been a number of different studies that have looked at risk management and the perception of risk related to collaboration management (Grudinschi et al., 2014, Thomson et al., 2009, Huntgeburth, 2015, Hon et al., 2012). The effect of trust on relationship risks in partnerships, how communication affects risk management and the effect of organizational structure on the perception of relationship risks are all examples of how different factors can have an effect on risk management and risk perception (Grudinschi et al. 2014). Unfortunately, according to Grudinschi et al. (2014 p.83) ‘risk perception and relationship risk management are rarely highlighted in discussions of public procurement and collaboration’.

According to Protection Motivation Theory (PMT), a common theory that is related to risk perception and risk tolerance, people will protect themselves when they perceive a risk; they

try to avoid negative consequences and feel that they have the ability to carry out preventative measures. When this theory is applied to this study, where there is an increase in risk perception the use of protective action increases, which is not adopting the public cloud for sensitive data and critical systems.

Basically, the PMT theory suggests that there is a relationship between risk perception and injury and that an organisation will take action if they are motivated and have the means (Campbell Institute, 2014). The means to prevent injury in the case of a government adopting the public cloud would be achievement of an acceptable level of governance or security and privacy, however, if they do not have these means then there will be increased risk perception. Therefore, there is a link between risk as a relationship factor and governance or security as cloud factors where the latter influences the former.

Another theory to consider in relation to the issue of risk perception that can provide an explanation about why governments are reluctant to place sensitive in the public cloud is Risk Compensation / Risk Homeostasis Theory. This theory basically states that a person will take more risk when there is greater security; risk taking behavior is directly related to the safety measures that are in place (Campbell Institute, 2014). If this theory is applied to the present study then it would suggest that a reason why governments are not taking the risk to place sensitive data in the public cloud is because there may be the perception that there are not enough measures in place in the areas of governance, compliance, security and privacy to secure sensitive data and critical systems. Again, there is a link between risk and cloud factors.

3.3.2.2 Link between Risk and Cloud and sub Cloud CSFs

An example of where risk perception has a link with a cloud CSF is that governments need a certain level of governance or control over the data not only for security purposes but also because it is required by legislation and regulation, without this there is an increased perception of risk.

In reference to the risk compensation theory, discussed in the above, there is a clear relationship between what the cloud provider is willing to offer such as governance, compliance and security and privacy and how secure they are as cloud critical success factors, and the government’s perception of risk with these factors. Therefore, there is

justification for considering both relationship and cloud factors together towards understanding the reasons why governments do not have confidence in the public cloud.

Brender and Markov (2013) have identified that the most important risks are related to information security, confidentiality of data and privacy. For government, this link between risk and security is especially a problem in the cloud where privileged user access associated with the processing of sensitive data bypasses the personnel controls that an IT department would normally have and therefore, there is the concern about malicious insiders of the cloud service provider, this is a sub cloud factor of governance and security and privacy. As a CSF, a way to reduce the risk perception here is to have sufficient information and assurances on who is hired and there must be the use of the least privileged principle whereby processes, individuals or entities have the minimum access to carry out tasks.

In consideration of the issue of risk, where there is a lower level of risk perception there will be more confidence to use the public cloud. Therefore, a lower perception of risk is considered a critical success factor in the relationship towards increasing confidence in the public cloud.

Moreover, this section has shown that risk cannot be considered in isolation, there is a relevant link between risk as a relationship CSF and cloud CSFs such as security and privacy and compliance, and sub Cloud CSFs such as knowledge and control over CSP employees. Therefore, the questioning in the research will consider the relationship between risk and factors of the cloud that are determined by risk perception.

3.3.3 Collaboration (CSF)

Collaboration between the government and the CSP has been shown to be necessary for governments to deploy to the public cloud. Specifically, collaboration is required for achieving CSFs such as governance and compliance. The government – CSP relationship is not something that takes place in one instant but rather takes place on an ongoing basis as requirements change, and therefore, the ability to collaborate with the cloud service provider is an essential relationship CSF.

3.3.3.1 General Theories and Ideas about Collaboration

Research into collaboration and partnership in public service sector procurement has received much interest and has been studied from different perspectives including efficiency, effectiveness, performance and success; however, according to Grudinschi et al. (2014) there

have been few studies that specifically focus on procurement in public sector procurement itself.

Collaboration is one of the important areas in order to provide high quality services and although collaboration practices and relationships have evolved in this area, there is still difficulty in gaining fluent collaboration between partners (Grudinschi et al. 2014). More specifically, collaboration fluency is a newly defined concept, similar to collaboration effectiveness, and takes into account managerial indicators which include identifying common goals and challenges (Grudinschi et al. 2014).

Collaboration efficiency refers to the cost of collaboration and collaboration effectiveness is about evaluating the ways that objectives are achieved from a managerial perspective (Grudinschi et al. 2014). Collaboration is a much broader concept and involves economic, operational and managerial indicators. Finally, there is concept of collaboration success which is related to satisfaction or dyadic sales (Grudinschi et al. 2014).

According to Thomson et al. (2009) there are five areas of collaboration that have emerged from the literature, these are governance, administration, organisational autonomy, mutuality and norms.

Governance is the decisions about the rules that will govern behavior and the relationship should be made jointly by both parties for there to be successful collaboration (Thomson et al. 2009). Specifically, this involves establishing a set of rules about who is authorised to make certain decisions, which actions are allowed and which are not and what information has to be provided.

Administration is the administrative structure that is required to move from governance to action, here the focus is on implementation and management as opposed to governance where the focus is on institutional supply (Thomson et al. 2009). However, this implementation in collaboration is not easy to achieve because of the autonomous or semi-autonomous nature of the relationship whereby traditional mechanisms for coordination, such as hierarchy, do not work (Thomson et al. 2009).

Partners have a dual identity, on the one hand they have their own identity and organisational authority, and on the other they have a collaborative identity. Therefore, there is a conflict between self-interests in wanting to achieve their own missions and maintaining an identity that is distinct from the collaboration and the collaborative interests which include achieving

collaborative goals (Thomson et al. 2009). Problems arise from the fact that there is no formal authority hierarchy between the partners.

Based on the idea of interdependence, mutuality means that each partner in the collaboration should enjoy mutual benefits according to their different interests or shared interests (Thomson et al. 2009). Mutuality occurs where one party has resources such as skills or expertise that the other party could benefit from.

Mutuality is also based on the idea of reciprocity, that in collaboration each party has a reciprocal obligation to each other and they expect that their contribution will be reciprocated by the partner (Thomson et al. 2009).

3.3.3.2 Link between Collaboration and Cloud Critical Success Factors (CCSFs)

In reference to the governance mentioned in the above, governance is clearly related to the governance that is referred to in the literature about government and cloud provider relationships where government require a certain level of governance over data and systems in order to comply with their own laws and regulations. Having the authority to make certain decisions, establishing who is allowed to do what and rules about sharing information are found in cloud provider and customer relationships, especially under the area of governance. Moreover, the process of governance is ongoing, there should be continuous negotiation to establish an equilibrium where although conflict may still occur marginally, there is still agreement on the rules for a collaborative environment achieved by managers understanding the agreed shared responsibility (Thomson et al. (2009). Therefore, there is clear association between collaboration as a relationship CSF and governance as a cloud CSF, moreover, this association applies to other cloud and sub cloud factors.

This link is further evidenced by an important idea raised by Alruwaili and Gulliver (2014) that was collaboration in detection. This idea is related to governments and the control of the data and includes the extent or ability of control of the data or specifically the extent of involvement and control over the detection of intrusion.

Collaboration refers to the ongoing relationship that the government has with the cloud provider when the government deploy sensitive data and critical systems to the cloud. Governments need to be confident that there is collaboration between the two parties in order to achieve the cloud related critical success factors of governance, compliance, security and privacy and performance and offering. As an example, a link between collaboration and

governance is where the government need control over data in order for there to be collaboration in detection of malicious behavior.

As collaboration is an overall relationship requirement it can be easily linked to the cloud CSFs and the literature has shown this. According to Marudhadevi et al. (2014) collaboration is important for the continuous checking that service provisions in the SLA are met which is a sub cloud factor for all four of the cloud critical success factors (governance, compliance, security and privacy and performance and offering). For example, a cloud sub factor of compliance is 'continuous auditing and assessment' and a cloud sub factor of security and privacy is 'Continuous monitoring of policy adherence and performance' both of which require collaboration as a relationship CSF.

Allocation of responsibilities is another important aspect of the service level agreement. It is important to ensure that all of the employees of the cloud service provider understands their duties and responsibilities in order to ensure that there is no conflict between them. Moreover, allocation of duties is important to achieve governance because the government wants to ensure governance is adhered to through the allocation of duties and responsibilities.

An effective system for ensuring collaboration, a relationship factor, requires clarity of roles and responsibilities, a sub cloud factor, as a mechanism to measure each other's activities especially in terms of roles and responsibilities, and communication in order to enhance the coordination, however, these can be difficult when the communication is relational and not routinised (Thomson et al. 2009). These factors reflect the sub cloud CSFs, for example, where the cloud factor is governance the associated sub cloud factor is clarity of roles and responsibilities, is also required to achieve the other cloud factors such as compliance and security and privacy.

Collaboration has been shown to be a universal relationship CSF and has been shown to be required in order to achieve all of the cloud CSFs. Collaboration is required for an effective ongoing relationship and if it is not achieved then there can be many occurrences that would lead to a decrease in the confidence of government to use the public cloud.

3.3.4 Negotiation (CSF)

The ability to negotiate is important for governments to achieve what they require from the relationship with the cloud service provider. This is a relationship CSF that is required to achieve all of the cloud and sub cloud factors. Without effective negotiation government will

not be able to, for example, achieve their governance and compliance requirements and therefore, will not be confident to use the public cloud.

The most important aspects of negotiation that are considered in this study are the ability to specify requirements and to have those requirements understood by the CSP. If a government feels that they do not have the ability to specify their cloud requirements or that their requirements are not understood then they will be concerned that their requirements are not met leading to a decrease in confidence.

As an aspect of cloud negotiation, being able to articulate or specify requirements properly is important for both the cloud customer and the cloud service provider and is something that will form the central element of the contract (Johansson and Lahtinen, 2012). Being able to articulate and specify requirements is especially important in the case of government and the public cloud because requirements specification should be clear, particularly because governments require a customised non-standard service from the provider. Furthermore, specified requirements are useful for analysing the procurement situation and auditing against agreed requirements. Alruwaili and Gulliver (2014) and Johansson and Lahtinen (2012) say that the articulation of requirements is important in the specification of contractual obligations in areas related to technical specifications for security and sensitive data.

3.3.4.1 Link between Negotiation and Cloud CSFs

Negotiation is a relationship critical success factor that is required in order to achieve all of the cloud critical success factors. Negotiation is where terms and conditions for the cloud are requested and agreed upon. Without effective negotiation, by both the government and the CSP, cloud factors as CSFs will not be achieved. Specifically, where the government has an inability to specify their requirements, or the CSP has an inability to understand those requirements, there is a failure in negotiation and an associated failure to achieve cloud requirements.

3.3.5 Reputation (CSF)

The reputation of the cloud service provider will play an important role in whether the government trusts the cloud service provider, perceives a risk and ultimately have confidence in the public cloud. Reputation or the perception of reputation has been chosen as a critical success factor because reputation is directly related to confidence to adopt the cloud (Burda

and Teutberg, 2014). Pilevari et al. (2013) say in reference to user satisfaction that there should be positive perception of reputation which is positively linked to trust.

3.3.5.1 General Theories and Ideas About Reputation

A justification for considering the information and knowledge that the government as a cloud customer has about the cloud service provider can be found in bounded rationality theory. This theory assumes that the rationality of the customer is bounded by the information and knowledge that they have to make decisions (Huntgeburth, 2015). Moreover, another important issue that highlights the importance of reputation in the government – CSP relationship is that although the user depends very much on the cloud provider, they have very little information about them (Huntgeburth, 2015). This issue is raised in consideration of the Principal Agent Theory whereby one of the problems of making an 'adverse selection' is the fact it is difficult to verify quality in relation to the CSP and their service, therefore, it would be reasonable to expect the government to rely on reputation in this case.

Although trust can be enhanced by the satisfaction of the user, trust can also be enhanced by the provider's reputation and the extent to which the client believes that the provider is genuinely concerned about clients (Burda and Teutberg, 2014). Trust can be enabled in an unknown entity through direct interaction, reputation and recommendation (Abbadi and Alawneh (2012). Huntgeburth (2015) talks about principal agent theory and social influence which also consider unknown entities and their reputation. Moreover, trust concerns can arise from the fact that customers have insufficient information about their cloud service provider (Alruwaili and Gulliver, 2014). Ryan and Falvey (2012) say that trust is based more on perception than fact.

It is important to consider the fact that the service relationship between the government as a user and the CSP takes place in a specific social context. One of the criticisms of the Principal Agent Theory is that it does not consider that the principal – agent relationship takes place in a social context. A response to this issue has been the Social Influence Theory which considers the context or the environment of the exchange relationship (Huntgeburth, 2015). In reference to reputation, according to Wiseman et al. (2012) a higher density in the social network of principal agent relationship, the more likely the principal will defer to the social network for assessing the cloud provider or monitoring their behavior. In the present study, this social network would include other users and networks of users that come together to help each other evaluate and even certify CSPs. Thus, it is important to question the

government about reputation, where information is received from other parties in the same social context and whether reputation is an influencing factor when considering adoption of the public cloud.

Similarly, Firdous (2011) says that trust is based on prior knowledge and experience. According to Alruwaili and Gulliver (2014) reputation includes assessment of cloud provider including security detection and prevention. There should be sufficient information about the cloud service provider - however important to note that the associated risk of insufficient information about cloud service provider can be mitigated through a detailed SLA (Alruwaili and Gulliver, 2014).

Norr et al. (2016) says that social psychology theory tells us that trust assessment of an unknown entity can be influenced by known entities who recommend it and that reputation is affected by the different entities opinions that can impact, negatively or positively an unknown entity's reputation.

Therefore, there is support for the idea that there needs to be consideration of the perception of reputation, in further support of the fact that reputation should be considered as a relationship CSF for confidence in the public cloud.

Although there is a clear link between trust and reputation, reputation is considered in this study because it is a relationship factor that has a strong impact on the decision of whether or not government should deploy to the public cloud. Before a government enter into a relationship with a CSP often reputation is one of the few types of information on which they can base their decision, or they form a perception of reputation after having experience or relationship with the cloud service provider.

3.3.5.2 Link between Reputation and Cloud Critical Success Factors (CCSFs)

Where there is the perception of a poor reputation in any of the cloud CSFs there will be a lack of confidence in these factors. Therefore, reputation is a relationship critical success factor that is required in order to achieve confidence in all of the cloud critical success factors. Reputation is a way of establishing credibility of the CSP in terms of issues such as security and control over data (Ahmed and Hossain, 2014) and a way to validate cloud attributes generally (Huang and Nicol, 2013)

Reputation has been established as a relationship CSF that has an effect on the confidence in all of the cloud critical success factors. To understand how reputation plays a role in relation to government confidence in the public cloud and which areas of the cloud are particularly affected this association is important. For example, it would be considered a factor for success in terms of having confidence in the public cloud if the government perceived a positive reputation about the security and privacy capability of the public cloud service provider.

3.4 Cloud Critical Success Factors (CCSFs)

In examining a relationship where governments do not have confidence to move sensitive data and critical systems to the public cloud, not only is it important to investigate the relationship factors such as perception of risk or negotiation as in the previous sections, but it is also important to investigate the cloud factors that are associated with the relationship factors. In consideration of the fact that the study looks specifically at government, the public cloud and sensitive data and critical systems, the adopted cloud factors in this study are chosen based on the fact that they have a direct link with governments concerns and include general factors that are also a concern for all organisations, and more specific factors that may be of particular concern to government such as governance and compliance. In fact, all cloud factors are relevant and of utmost importance for a government considering the public cloud.

3.4.1 Governance (CSF)

One of the main issues that governments face considering deployment to the public cloud is governance. Governance refers to the level and type of control that governments have over their data and systems that are deployed to the cloud. The more governance that a government maintains the more likely they will be confident to deploy to the public cloud (Haag et al., 2014, Nycz and Polkowski, 2015, Diez and Silva, 2013).

Due to the nature of the public cloud, that it is provided by a third-party provider and hosted on a third-party platform, there is a loss of governance of the owner of the data, unlike private clouds where the physical infrastructure is under the direct control of IT departments, there are no other parties involved and they can secure the servers with a firewall. However, with a public cloud most of this control is lost, there are other parties involved which include the cloud provider (CP) and the cloud service provider (CSP) and the cloud is shared by multiple

tenants (Jansen and Grance, 2011, Takabi et al., 2010). This is further supported by the ENISA Security & Resilience in Governmental Clouds report (ENISA, 2011) that says that it is challenging for public bodies to manage their security requirements in traditional IT environments and this problem is made worse in cloud environments because they have to understand that there is a shift in the balance of accountability and responsibility for functions such as governance and control of IT and data operations (ENISA 2011). Thus, there has been a shift to indirect governance and control over IT infrastructure and data, this is especially the case with PCC and SaaS deployments, although these issues can be overcome by effective negotiation with the provider (ENISA, 2011).

According to Kanwal (2014) continuous access to data is required under all situations and cloud architecture is different from traditional IT infrastructures and therefore, availability of data is more crucial. Ownership and control of data should remain with the customer as much as possible, this is achieved through process execution and data ownership. Process execution control ensures control over activities and processes performed on applications by cloud providers, if an organisation has sensitive data or critical applications in the cloud they would prefer themselves to have a high level of control in the processing of the applications. Data ownership refers to where there is a need for the customer to feel that they still own the data and that it is not owned by the cloud provider. Ownership guarantees data is under the control of the organisation and only authorised entities can access the data. Data ownership includes access control policies which define access rights in the cloud (Kanwal, 2014).

An additional consideration in the public cloud is the employees of the cloud provider and cloud service provider, over which government require a level of governance (Brender and Markov, 2013, CSA Guidance, 2011). There is a loss of control and concerns related to the employees of the CP and the CSP and there are implications for backup, disaster recovery and security. Firdhous et al (2011) say that there is a multiple stakeholder problem because of open space security and mission critical data handling issues. Some of the responsibilities for administration and operations are delegated to the cloud provider, and even though the customer would like to have the same type and standard of service that they would have if they hosted the cloud themselves, the cloud provider will have a different policy. Moreover, because there are three main parties involved in PCC, namely; the cloud provider (CP), the cloud service provider (CSP) and the cloud customer (CC), there will be a change in the level and type of governance that a government has.

One of the issues raised in the Principal Agent Theory, that is a cause of the 'adverse selection' issue highlighted by the theory, is that in a cloud service relationship it is very difficult to verify quality. However, governments need a certain level of knowledge and control over data and systems in order to have an effective principal – agent relationship. Another relevant problem that is raised in the Principal Agent Theory is that it is very difficult to monitor the actions of the provider; this would clearly be an issue for government in terms of the required governance. According to the positivist agency theorists the way to resolve this problem, which could lead to a 'moral hazard', is to establish a bilateral governance mechanism between the user and the CSP (Huntgeburth, 2015).

The cloud is characterised by multi-tenancy and each party has their own Security Management Process (SMP) that they want to enforce on the cloud assets, no individual stakeholder can control or maintain the entire security process of the cloud services because they do not have the required information or perspective, multi-tenancy means that different security requirements will have to be maintained in the same service (Almorsy 2011) and therefore, there is a loss of governance.

All of these issues lead to a decrease in the type and level of governance that governments have over the cloud and their associated assets. In reference to these issues, the change towards indirect governance and control over IT infrastructure and data through the use of the public cloud presents a significant challenge. However, some of these issues can be overcome by negotiation.

Governance has implications for other considerations of the cloud and the relationship between the cloud CSP and the government. In reference to trust, as part of establishing a trustworthy environment, Abbadi and Alawneh (2012) say that the cloud provider should not interfere with customer application data and should pass control over the data to the customer. Here a clear association between governance and trust is made.

The link between governance and trust has also been mentioned by Kanwal (2014) who said that control and ownership of data and applications stored in a cloud is very important to increase the level of confidence of cloud customers. Moreover, trust will be low if the customer does not retain much control over their critical assets in the cloud platform. Trust models increase this confidence through guaranteeing a level of data control through adopting authorisation and authentication mechanisms. This requires defined access rights or the

authorization, authentication and visibility of stored data at different physical locations. (Kanwal, 2014).

Additionally, the relationship between risk and governance is mentioned by Elena (2013) who says that risk management decision processes are significantly influenced by concerns about loss of governance. Moreover, risk perception significantly affects IT innovation strategies and risk perception is directly influenced by cloud computing applications (Elena, 2013). Therefore, risk as a relationship factors is associated, through influence, by cloud factors.

In order for government to achieve governance they have to be able to specify their governance requirements and have their governance requirements understood, this would lead to more confidence in the public cloud. Therefore, in order to achieve governance there is a need for effective negotiation and thus, there is a link between governance as a cloud critical CSF and negotiation as a relationship critical success factor (RCSF). This relationship has also been established in section 3.3.4 in consideration of negotiation.

Therefore, in addition to the general need that government have to retain a certain level of governance over data, in order to achieve for example compliance and security privacy, there is a clear link between governance as a Cloud Critical Success Factor (CCSF) and risk, trust, negotiation (ability to specify requirements and have requirements understood) and collaboration as Relationship Critical Success Factors (RCSF).

3.4.1.1 Sub Cloud CSFs of Governance

The relationship that a user has with a cloud service provider is something that takes place on an ongoing basis due to the way the service is provided. Therefore, there is a continuing reliance on the cloud service provider (Huntgeburth, 2015). This idea is reflected within the different cloud factors, specifically, the sub critical success factors of this study where there is consideration of an ongoing dependency on the cloud provider. Within governance these Cloud sub CSFs include knowledge and control over data, processes and applications, knowledge and control over third party issues, knowledge and control of CSP employees and auditing and measuring the CSP. These are factors that are important in an ongoing relationship.

In order to answer the research question of the study ‘Are there certain cloud related factors that are affected by relationship factors that may affect government confidence in the public

cloud?' it is necessary to consider the specific areas within each cloud factor. The reason for this is that the study wants not only to find out the relationship factors that affect government confidence in the public cloud but the specific areas of the cloud that are affected by these relationship factors. This will allow the researcher to identify the specific areas of the cloud that are an issue in the government – CSP relationship which may affect public cloud adoption. This approach would offer a greater level of insight, for example, if governments feel that they do not have the ability to specify governance requirements, it would provide more insight and be more useful to practitioners if it was discovered which specific areas of governance, such as control over data or control and knowledge of CSP employees, are affected by relationship factors.

Through a review of the literature and models for cloud adoption a number of sub cloud factors found within cloud factors are identified. If these are achieved, then it is considered that this is successful and there will be increased confidence in the public cloud.

Table 3-1: Cloud Sub Critical Success Factors (CSFs) - Governance

Cloud CSF	Cloud Sub CSFs
Governance	Data control (Kanwal, 2015). Data execution (Brender and Markov, 2013). Data availability (Kanwal, 2015). Knowledge of data location (Brender and Markov, 2013, (CAIQ) (v3.0.1). Process execution (Kanwal, 2015). Remote access control (Firdhous et al 2011). Accessibility (Norr et al. 2016). Control over definition of access rights (Norr et al. 2016). Accountability over deployed applications and systems (Jansen and Grance, 2011). Control over transfer of data (Brender and Markov, 2013). Continuous access during all situations – normal and disaster (Kanwal, 2015). Clear ownership rights over data (Jansen and Grance, 2011). Knowledge of movement of data within the cloud (CSA Guidance). Knowledge of who has control over data (CSA Guidance). Collaborative governance structures (CSA Guidance). Knowledge and control over CSP employees (Brender and Markov, 2013, CSA Guidance) . Control over other tenants in cloud (Jansen and Grance, 2011) (Access control) Takabi et al (cited in Alhamad et al 2010). Not share cloud resources with competitors (other tenants) (Almorsy, 2011).

	Clarity of roles and responsibilities (Jansen and Grance, 2011). Alignment of policies regarding assignment of roles (Jansen and Grance, 2011). Transparency of CSP actions (Firdhous et al 2011). Knowledge of third party relationships (Alhamad et al. 2010, Firdhous et al. 2011). Control over third parties (Takabi et al (cited in Alhamad et al 2010). Third party identity management (Takabi et al (cited in Alhamad et al 2010). Trust in supply chain (CSA Guidance). Policy integration with third parties (Takabi et al (cited in Alhamad et al 2010) (Jansen and Grance, 2011). Multiple distributed clouds used by CSP – trust relationship required between customer, CSP and CPs (Fan and Peros, 2014). Security requirements aligned between three parties (CP, CSP and customer) (Almorsy, 2011). Do CPs understand security requirements (Almorsy, 2011) Duality in trust (Kanwal, 2015). Dynamic SLA (Kanwal, 2015). Measuring other parties activities (Kans, 2012). Framework to monitor and measure risk (CSA Guidance). Clarity of who will have access to data (CSA Guidance). Mechanism for vetting those who have access to the data (CSA Guidance). Clarity of what activities for what type of information (CSA Guidance). Clarity of which users for which type of information (CSA Guidance). Control over security policy (Ahmad and Janczewski 2011). Direct point of contact in CSP (Jansen and Grance, 2011). Maintaining situation awareness (in order to weigh up options and set priorities) (Jansen and Grance, 2011). Ability to enforce control and maintain accountability (Jansen and Grance, 2011). Auditing mechanisms for data storage, protection and use (Jansen and Grance, 2011). Organisational practices (government) followed by CSP throughout system lifecycle). Adequate oversight to maintain accountability (Jansen and Grance, 2011). Control over deployed applications (Jansen and Grance, 2011). Sufficient recourse to address and resolve problems (Jansen and Grance, 2011). Sufficient risk mitigation through negotiated SLA (Jansen and Grance, 2011). Governance during migration to the cloud (Estonia Report).

Table 3.1 illustrates that there are numerous cloud sub factors to be considered. This study should consider sub cloud factors of cloud factors towards understanding the government – CSP relationship, however, from a practical perspective they are too numerous for all of them to be included in the questionnaire. Therefore, the sub cloud factors are consolidated to

reduce the number of variables in the questionnaire, illustrated in Table 3.2 as relevant cloud sub cloud factors of governance.

Table 3-2: Summarised Cloud sub Critical Success Factors (CSFs) for Governance

Governance – Cloud sub CSFs	**Description**
Knowledge and control over data, processes and applications.	In order for the government to achieve a required level of governance they need a certain level of control over data, processes and applications and at least knowledge of what is taking place regarding these.
Surety of other cloud tenants.	Government need a certain level of control other cloud tenants or at least be assured of security and control by service provider and be assured.
Knowledge and control over third party (CP) issues.	Government require certain level of control and knowledge of the Cloud Provider (CP) as a third party.
Clarity of roles and responsibilities / accountability (government and CSP).	Important to know who is responsible for what in order to achieve governance.
Dynamic SLA (towards mitigating risks, adapting to changing requirements).	Governance requirements can change so a corresponding dynamic agreement is required.
Control and knowledge of CSP employees.	In order for the government to achieve a required level of governance they need a certain level of control over employees at the cloud service provider.
Auditing and measuring of CSP.	Auditing, monitoring, measuring of CSP performance, activities and risk.
Collaboration.	To ensure that governance is achieved both parties need to collaborate.
Governance during migration to the cloud.	When sensitive data and critical systems are migrated to the cloud the government are required to have governance.

3.4.1.2 Summary

It has been shown in the above that a lack or a loss of governance as a cloud critical CSF and sub cloud CSFs, which governments have over data and applications is linked to trust and the perception of risk as relationship CSFs in the public cloud. Therefore, a cloud critical success factor in this study is an acceptable level of governance that would decrease risk perception and increase confidence in the public cloud.

These links are the justification for investigating both the relationship critical success factors and the associated cloud critical success factors when investigating the relationship reasons that governments have for being reluctant to deploy to the public cloud.

3.4.2 Compliance (CSF)

The physical component of the public cloud is often located outside of the sovereign territory of a government that uses it; this gives rise to legal issues. Firstly, there are the legal issues that are related to the governments domestic laws such as those related to personal data of citizens and the legality of whether or not it can be stored on a server in another legal jurisdiction, and secondly, the laws of host countries whereby a country may have laws where they can subpoena data for investigation purposes, for example, in the United States a cloud provider can provide user information to a public authority which seriously diminishes the user's data security (Ahmad and Janczewski, 2011). Therefore, there would be a perception of a risk to privacy of citizen data. In this situation where local authorities have to gather data for forensic purposes, users will be deprived of their privacy; examples of this include the Patriot Act in the US and the UK Regulation of Investigatory Powers Act 2000 (Ahmad and Janczewski 2011). These legal issues are important considerations because they relate directly to the control that governments have over citizen data, and are particularly a concern is security for more sensitive data and critical applications (Ahmad and Janczewski, 2011).

Although a government would be justified in expecting that their data is protected in another third-party jurisdiction, there is no guarantee that international legal protection would be respected, there are however, international conventions that could protect this (Microsoft, 2016A), for example, the Vienna Convention on Diplomatic Relations (VCDR) and/or the Vienna Convention on Consular Relations (VCCR) (Estonia Ministry of economic Affairs and Communications, 2013).

However, local laws where the cloud provider is located may not protect the security and privacy rights of the user, and it may be impossible for the cloud provider and the user to comply with auditing and the law because each party is in a different jurisdiction. Clauses included in agreements by the providers of public clouds often say that terms of the agreement can be changed at their discretion and it is therefore important for the government in order to be compliant to remove these clauses from the contract in order to maintain compliance (Australian Government, 2011).

Moreover, there are restrictions of where the data can be located, for example, the EU Directive 95/46/EU does not allow data to be transferred outside of the EU (Ahmad and Janczewski 2011). There are also issues related to contractual obligation whereby the cloud provider may contractually prohibit the user from migrating to another cloud (Ahmad and Janczewski 2011).

3.4.2.1 Sub Cloud CSFs of Compliance

In order to answer the research questions of the study, it is necessary to consider the specific areas within each cloud factor.

Table 3-3: Cloud Sub Critical Success Factors (CSFs) - Compliance

Cloud CSF	Cloud Sub CSFs
Compliance	• Security and Privacy. • Multiple stakeholders. • Third party CP. • Regulatory compliance – EEA (European Economic Area data protection laws --- government remain responsible not third party --- MAIN ISSUE location of data in public cloud must comply with privacy regulations in different jurisdictions (example of high risk when other governments pass laws to access data – e.g. supeona US) Patriot Act (Brender and Markov (2013). • Continuous review and assessment of service regarding government requirements to ensure contract adherence (Jansen and Grance, 2011). • CSP understands laws and regulations that impose security and privacy obligations (Jansen and Grance, 2011) (specifically – data location, privacy and security controls and records management). • Account for different legal jurisdictions (CSA Guidance). • Overcome issue of cloud being borderless with different jurisdictions and different laws – to establish compliance (ENISA 2014). • Governments prohibit or restrict data to be transferred outside country – like EU so servers have to be in EU. • Data location. • Investigative support. • Provider lock-in (also relates to endurance / or going out of business / takeover and this all links to ADV CONT This inform a CSF domain which may be under ADV CONT maybe on its own. • Confidentiality. • Auditability. • Must understand risks and define controls before sensitive data is placed in the cloud. • CSF ability to identify risks and associated controls relevant to the IT function that will be migrated to the cloud (Brender and Markov (2013). • Provider lock in (Brender and Markov (2013). • Auditability (Brender and Markov (2013). • Clarity on jurisdiction for arbitration (Brender and Markov (2013). • Data destruction (Brender and Markov (2013). • Data traceability and monitoring of irregular activities ---- when migrating data to cloud in electronic format it can be downloaded to a usb. • Security during data transfer. • Physical security and natural disasters,

	• Articulate requirements – buyer and supplier – specifications should be clear (Johansson and Lahtinen, 2012), • Allocation of responsibilities – cloud employees understand duties (Kans, 2012). • Security of provider assessed against security management of user (CSA Guidance). • Consistency in risk management (CSA Guidance). • Survivability of provider (CSA Guidance). • How data is managed during transfer (during business continuity) (CAIQ) (v3.0.1). • Ability to define geographic locations of data procedure (CAIQ) (v3.0.1). • Data not migrated beyond acceptable geographic boundaries (CAIQ) (v3.0.1). • Clarity about which jurisdiction applies to the data (ENISA, 2011). • Local laws where CP operates protect interest of customer (Ahmad and Janczewski 2011). • Compliant firewalls (Continuity central). • Clarity of roles and responsibilities (managing risk and ensuring organizational requirements) (Jansen and Grance, 2011). • Ability to act with laws, regulations, standards and specifications – at national and local levels (Jansen and Grance, 2011). • Understanding of CSPs technology and implications it has for compliance (Jansen and Grance, 2011). • Sufficient risk mitigation through negotiated SLA (Jansen and Grance, 2011). • Compliance when migrating to the cloud (Estonia Report).

Again, from table 3.3 above it can be seen there are numerous sub cloud factors to be considered and too numerous to be included in the questionnaire. Thus, the sub cloud factors have been summarised and consolidated as shown in Table 3.4 as relevant cloud sub cloud factors of compliance.

The nature of the relationship between the government and the CSP has the unique characteristic of being on an ongoing basis, unlike with the purchase of software which is often a one-stop relationship with some after sales service. Compliance and the various sub aspects of compliance require attention on an ongoing basis.

Table 3-4: Summarised Cloud Sub CSFs for Compliance

Compliance CSFs	**Description**
Continuous auditing and assessment	Can continuously assess and monitor the CSP for adherence to compliance.
Clarity and confidence regarding jurisdiction	Clarity of law for arbitration, confidence that jurisdiction achieves compliance.
Data management	Includes transfer and location of data.
Roles and responsibilities	Allocation and clarity of roles and responsibilities.
Security and privacy	Defined security controls, identification and management of security risks.
CSP ability to be compliant with government laws and regulations	Ability to comply with laws and regulations, understand technology and implications for

	compliance.
Confidence related to location of data	U.S. subpoena.
Compliance when migrating to the cloud	The ability of the CSP to remain compliant when data in being migrated to the cloud.

3.4.2.2 Summary

Governments are bound by regulation and law because they are responsible for the data of their citizens as well as highly critical government data on which the security of the state depends. The lack of governance has been shown to be a concerning factor for governments considering the public cloud. Therefore, achieving the required type and level of governance has been considered a critical success factor where its achievement will bring confidence in the public cloud.

3.4.3 Security and Privacy (CSF)

Security and privacy is one of the main concerns that governments have when considering the public cloud. Security and privacy in cloud computing does not have a good reputation and has been the main reason that critical sectors such as healthcare and banking have been reluctant to use the public cloud, this is made worse by the fact that governments are not aware of the security mechanisms of their cloud service providers (Bamiah et al., 2012).

Security has wide reaching implications and considerations from the prevention of malicious intruders to ensuring security in the cloud provider and cloud service provider. Each of the three parties, cloud customer, cloud service provider and cloud provider as a third party, have their own security requirements which may in fact conflict with each other, in other words each stakeholder has different security requirements that they want to impose on the same service (Almorsy, 2011). Alam et al. (2013) say that security has implications for user access, regulatory compliance, data location, data segregation, investigative support, recovery and long term viability.

Although there are numerous advantages to the cloud, if security is not achieved then these advantages are worthless (Ahmed and Hossain, 2014). The main issue is that government data and systems are to entrusted to what is essentially a public internet, data storage where there is multiple tenancies and governments lack control and the traditional security controls of authorisation and authentication are not sufficient (Hashizume et al. 2013). There are a

number of different areas that need to be considered in relation to security and include the network, host, applications and data (Zwattendorfer et al., 2013, Hashizume et al. (2013).

Where IT adoption theory does consider security it often considers security in a general and abstract level, however, there is neglect in the IT adoption theory where it does not consider that concern about security, especially in a cloud service relationship, is more weighted and specific which leads to organisations deferring their cloud adoption (Huntgeburth, 2015).

Security and privacy is linked to negotiation because governments should be able to specify their security and privacy requirements and have them understood by the CSP. Furthermore, governments, as part of compliance and governance requirements need to be involved in security management processes, be aware of third party activities in this area, be able to vet the employees of service providers and have transparency and clarity of roles and responsibilities. In reference to a link between security and privacy and collaboration, all of these requirements need collaboration as a relationship CSF.

3.4.3.1 Sub cloud CSFs of Security and Privacy

In order to better understand the issues within the relationship that may have an effect on the willingness to adopt the public cloud, the sub cloud factors of security and privacy are considered in the investigation of the government – CSP relationship. The sub cloud factors of security and privacy are presented in Table 3.5.

Table 3-5: Sub cloud Critical Success Factors (CSFs) - Security and Privacy

Cloud CSF	**Cloud Sub CSFs**
Security and Privacy	Identity and access management – authentication, authorization (Jansen and Grance, 2011). Ability to specify security requirements (Almorsy). Sufficient involvement in the security management processes of the CSP (Almorsy). Awareness of security efforts by third party (CP) (Jansen and Grance, 2011). Different security policy for different types of data (sensitivity) (CSA Guidance). Offered encryption when data moving through public network (CAIQ) (v3.0.1). Continuous monitoring of security performance (Almorsy, 2011). Continuous monitoring of security policy adherence (Almorsy, 2011). Effective disposal of hard drive (Kidman, 2013).

	Protection against data loss (Venkatraman, 2014). Protection against shared technology vulnerability (Venkatraman, 2014). Protection against malware on IaaS (Venkatraman, 2014). Protection against malicious insiders (CSP, CP) (Venkatraman, 2014). Protection against DOS attackes (Venkatraman, 2014). Secure interfaces and APIs (Venkatraman, 2014). Rapid response against attack. Data access (Estonia Report). Data handling (Estonia Report). Data lifetime management (Estonia Report). Data access auditing (Estonia Report). Separation of duties and least privilege (Estonia Report). Isolation of tenant applications (Jansen and Grance, 2011). Vetting employees (Jansen and Grance, 2011). Being notified of breaches (Jansen and Grance, 2011). Compliance with laws and regulations (Jansen and Grance, 2011). Assured about security related to multi-tenant environment (Jansen and Grance, 2011). Understanding of virtualization and isolation employed by CSP and the risks involved for the government (Jansen and Grance, 2011). Sufficient risk mitigation through negotiated SLA (Jansen and Grance, 2011). Assured about security for internet-facing service (Jansen and Grance, 2011). Clarity of roles and responsibilities (managing risk) (Jansen and Grance, 2011). Understanding of CSPs technology and implications it has for security (Jansen and Grance, 2011). Transparency of CSP and CP security and privacy controls – to assess risk (Jansen and Grance, 2011). Security and privacy when migrating to the cloud (Estonia report).

From Table 3.5 above it can be seen there are numerous cloud sub factors, too many to be included in the questionnaire. As with governance and compliance the factors have been summarised and consolidated as shown in Table 3.6 as associated sub cloud factors for security and privacy.

Continuing with idea that the relationship between the government and the CSP is an ongoing bilateral exchange, the sub cloud CSFs of security and privacy reflect what is required in this type of relationship, these include the continuous monitoring of policy adherence, sufficient involvement in security and surety regarding CSP employees. All of the factors are important in an ongoing relationship to ensure government confidence in the public cloud. Therefore, in order to achieve these sub cloud CSFs a negotiation and collaborative relationship between the government and the CSP is required.

Table 3-6: Summarised Sub cloud Critical Success Factors (CSFs) for Security and Privacy

Security and Privacy CSFs	**Description**
Security of third parties.	Requires encryption.
Continuous monitoring of policy adherence and performance.	The CSP continuously monitors security adherence and provides updates to the customer.
Sufficient involvement in security.	Government employees allowed to be directly involved in security and privacy within CSP organization.
Tailored security and privacy policy for differing needs.	These needs are related to a public cloud solution for government including consideration of sensitive data, critical systems, more permanent cloud solution government (including advanced digital continuity).
General – security and privacy provision.	Intrusion detection, encryption, data loss, malicious insiders, DOS attacks, security and privacy during migration to the cloud.
Clarity of roles and responsibilities.	Clarity about who is responsible for what, includes who has authorisation and access rights.
Surety regarding CSP employees.	Need for insider logging activity (ENISA, 2011).

3.4.4 Performance and Offering (CSF)

Performance and offering in this study refers to the standards of performance of the cloud service in terms of speed, efficiency and capacity, and offering in terms of the types of service that is available according to customer requirements. Governments have unique and specific performance and offering requirements due to their nature, and therefore, if these are achieved, they are considered as success factors.

According to Kanwal (2015) performance is related to detection of malicious behavior which is a high priority for cloud customers and quality of service transparency offered by the cloud service provider. Quality of service transparency is important because it helps the customer to

detect any deviation from their specifications in their agreement. Moreover, Pilevari et al. (2013) says that user satisfaction is strongly related to efficiency and performance which includes response time, usability, customization, adaptability, flexibility, inter-operability and scalable storage. Quality of service can be evaluated in two ways; firstly, by measuring quality of service attributes such as response time through port and network bandwidth and secondly, based on feedback. Di Modica (2014) says that is important that the cloud service provider offer support services whereby the cloud service provider helps customer to exploit the cloud to the full.

Another important aspect of performance and offering is availability of service and disaster recovery which should be established in the agreement (Brender and Markov, 2013). For disaster recovery, there are two situations to consider firstly, where the cloud service provider recovers in the case of a disaster, and secondly, customer recovery which is one of the main reasons or advantages for cloud adoption in the first place.

A pertinent issue related to performance and offering is provider lock-in and long-term viability. The agreement between the CSP and the customer should include provisions for the case of bankruptcy or takeover of the CSP or CP, during which time data should be available or it will be available to transfer to a replacement application or another provider.

In fact, long term dependency on CSPs is mentioned as an agency issue in Huntgeburth's (2015) Cloud Service Relationship Theory, this is because there may need to be a change in the CSP or the CSP may go out of business. In any case one of the considerations of the Cloud Service Relationship Theory is switching concerns and that is why end of service is addressed as a sub cloud issue in the examination of the relationship in the study under the performance and offering cloud factor.

The literature shows that one of the main issues with the cloud is that it offers a standardised service (Hon et al., 2012), which often means there is less room for more customisable solutions, something that a government would need in a cloud solution. However, for larger organisations that are regulated, which include governments and government departments, there should be increased negotiation in order to insist that requirements are met (Hon et al. 2012). Standardised offering is a problem and providers do not consider those who wish to pay for differing services, the result of this situation is that there is restriction and inflexible negotiation (Di Modica, 2014). Therefore, there is need for more refined SLAs based on

specific needs of customer which can be achieved through dynamic SLA management and negotiation (Di Modica, 2014). Thus, there is an opportunity for negotiation on requirements.

Services that are offered by the CSP do have an effect on the willingness to adopt the cloud. The literature, cited in the above, has shown that one of the main issues with cloud service offerings is that they are often standardised as cloud providers are offering a large scale. This is a problem that is recognised by the Principal Agency Theory and is applicable to the cloud service relationship. In the agent-principal relationship the government outsources cloud services to the CSP, and where the problems arise is either when the government as the principal does not have enough information about a CSP which would lead to what is referred to as 'adverse selection' (Huntgeburth, 2015), or where the CSP would not perform as they were expected to, this is referred to as the 'moral hazard' (Huntgeburth, 2015). The theory suggests that the interest of the CPS is to provide the service at a minimum cost, and therefore, the standardisation in the service may occur. The government on the other hand has different interests in this regard which includes a tailor-made service to suit their specific and unique requirements. Therefore, it is important to address performance and offering towards understanding the relationship between the government and the CSP and how this has an impact on the government's willingness to adopt the public cloud.

In order to ensure a tailored-made performance and offering and on an ongoing basis to achieve quality of service transparency continuously and monitor performance against the terms of a negotiated agreement, there is a need, therefore, for both negotiation and collaboration as relationship CSFs towards adoption of the public cloud. Moreover, this adherence to negotiated and agreed performance as a cloud critical success factor is also related to trust in the CSP that they will adhere to agreements and the perception of risk that they will not adhere to agreed terms and condition.

Therefore, there is an association between the need to negotiate, as a relationship CSF, the terms for performance and offering, as a cloud CSF, specifically, there is a need for governments to be able to negotiate a more customised cloud solution to meet government needs.

Moreover, it has been shown here that performance and offering is also linked to the need to collaborate where it is necessary for a government to monitor on an ongoing basis the service provision and performance in order to check if it complies with what has been established in agreements. Finally, the issue of standardisation can also be associated with the perception of

risk because if a service is standardised then there is the real risk that governments would not get what they require in terms of service and offering.

3.4.4.1 Cloud Sub Critical Success Factors of Performance and Offering

Towards answering the research questions and achieving the aims of the study, it is necessary to consider the specific sub areas of performance and offering as a cloud factor. These sub critical success factors offer further insight into the specific areas of the cloud that may be a concern in relation to relationship factors. The sub cloud factors of performance and offering are presented in Table 3.7.

Table 3-7: Sub cloud Critical Success Factors (CSFs) - Performance and Offering

Cloud CSF	**Cloud Sub CSFs**
Performance and Offering	Custom environment and negotiation of each provision (CSA Guidance). Ability to provide service in stipulated time (Jansen and Grance, 2011). Ability to provide service in stipulated cost (Jansen and Grance, 2011). All contractual requirements explicitly recorded in SLA (Jansen and Grance, 2011). Dynamic / flexible SLA (Jansen and Grance, 2011) (Kanwal et al., 2014). Sufficient risk mitigation through negotiated SLA (Jansen and Grance, 2011). Different security policy for different types of data (sensitivity) (CSA Guidance). Availability assured (Jansen and Grance, 2011). No conflict for key resources (Jansen and Grance, 2011). Offers business continuity (CAIQ) (v3.0.1). Understands continuity needs (CAIQ) (v3.0.1). Sufficient length of support cycle (for security and performance). Sufficient notice of disruption to applications (Kidman, 2013). Up to date applications (Estonia Report). Negotiable contract (Jansen and Grance, 2011). Additional service of specialized staff for specific security purposes (Jansen and Grance, 2011). Backup and recovery (Jansen and Grance, 2011). Continuous evaluation of SLA (Jansen and Grance, 2011). Support life cycle.

As with the previous sub cloud factors for the other cloud factors in previous sections, there are too many to be included in the questionnaire from a practical perspective. As with the other cloud factors in the above, the cloud sub factors have again been summarised and

consolidated, shown in Table 3.8, as relevant cloud sub cloud factors for performance and offering. This summarisation and consolidation allows the specific sub areas of the cloud to be addressed in the research of this study.

Again, because the relationship between the government and the CSP is an ongoing relationship, whereby it is IT as a service rather than IT as a product (Huntgeburth, 2015), this should be reflected in the sub cloud CSFs for performance and offering. In relation to this type of relationship the following cloud sub CSFs for performance and offering are important: a dynamic and flexible SLA, continuous monitoring of performance, additional specialised staff for government specific needs, sufficient support lifecycle, sufficient notice of disruption and end of relationship issues (see Table 3.8).

Table 3-8: Summarised Sub cloud Critical Success Factors (CSFs) for Performance and Offering

Performance and offering CSFs	**Description**
Customisable cloud environment.	Can the service be customised for individual service requirements?
Dynamic / flexible SLA.	Can the agreement change according to changing requirements on an ongoing basis?
Continuous monitoring of performance.	The CSP monitors performance against agreements.
Meet government specific requirements.	Time / efficiency / availability.
Additional specialised staff for government specific needs.	Security / governance / compliance.
Backup and recovery.	Disaster recovery / business continuity.
Sufficient support lifecycle.	After sales service / includes guaranteed and extended support.
Sufficient notice of disruption.	The CSP informs the customer in sufficient time of any disruptions to the service.
End of relationship.	Hard drive disposal.

3.5 Summary

This chapter has highlighted both the relationship and cloud factors that are pertinent to understanding and revealing potential issues in the government – CSP relationship that may influence adoption of the public cloud. The importance of these factors has been shown individually and in association with other factors, where it has been shown that there is an inextricable association between relationship and cloud factors, that need to be considered together to understand the relationship. The relevance of these factors in the relationship were explained and how they can potentially create negative intentions towards cloud adoption. Moreover, in particular reference to cloud factors, there was an explanation of the relevance of the individual specific sub cloud factors found within the general cloud factors.

Identifying and understanding the relationship, cloud and sub cloud factors was important towards the development of research methods, where they are applied in order to understand the relationship and associated cloud issues in the government – CSP relationship.

4 Methodology

Objectives

- **To present the methodological approach**
- **To show justification and development of adopted methods**
- **To show application of adopted methods**

4.1 Introduction

This chapter presents the methodological approach used in this study which includes a mixed methods approach using both qualitative and quantitative data. There is an explanation and justification for this research methodology in order to achieve the aims of the study and to answer the research questions. Moreover, the adopted methods are also introduced which include a questionnaire as the quantitative method and a semi-structured interview as the qualitative method. The justification, development and use of the questionnaire and the semi-structured interview is presented with an explanation of sampling, conducting the method and the approach for analysing the data. Finally, the ethical issues are also addressed.

It has been established that governments are reluctant to place sensitive data in the public cloud because of a number of concerns related to governance, compliance, security and privacy and service offering. These issues are negotiated between government and the CSP and the literature shows that there is currently a level of perception of risk and low level of trust in relation to cloud adoption. This study aims to reveal the relationship and associated cloud factors that are responsible for this of lack of confidence in the public cloud.

It is within the relationship between the government and the CSP that specific requirements of government are negotiated, specifically; these are the cloud related requirements such as governance, compliance and security which are negotiated in a relationship context. Therefore, cloud factors and relationship factors are inextricably linked, this has been established in the research design presented in Chapter 3, and need to be considered together in order to understand cloud concerns within the relationship. Moreover, relationship factors may affect the consideration of these cloud specific factors, and it is one of the premises of this study that the problem lies not only with the concerns about cloud-specific factors but in the relationship where those cloud factors are considered, negotiated and collaborated on. Therefore, the methodology will be developed to reveal the association between these relationship and cloud factors according to the established research design of the study.

It is these cloud and associated relationship factors that are considered in the development of the questions in the research methods. To provide an example, it is already known that governance is a major concern for governments in the public cloud; however, this study wants to find out how the associated relationship factors are relevant to this concern, whether, for example, there is a perception of risk or a perception of the inability to specify

requirements that are causing this concern, for example, because governments cannot specify their requirements or they do not trust the CSP.

4.2 Methodological Approach

Here the methodological approach is presented and justified as approach to achieve the aims and objectives and research questions of the study. The methodology is exploratory and includes a mixed methods approach using both quantitative and qualitative research.

4.2.1 Research Philosophy

In consideration of the research approach there needs to be consideration of the philosophical foundations. Because the study uses a mixed methods approach it is necessary to consider the research philosophy for each method.

A positivist philosophy is rejected in this study because there is the criticism (Crossan, 2003) that it does not provide a way of examining in-depth people and their behavior. This is due to the nature of man where it is impossible to establish laws and a positivist approach to research is basically about studying things as hard facts and that the relationships between these hard facts are established as laws (Crossan, 2003). People are not objects and they are open to feelings, opinions, perceptions and attitudes which would be rejected by positivists (Crossan, 2003). The present study is concerned with opinions and attitudes of the government personnel who are responsible for making decisions about the public cloud, therefore, the positivist approach is rejected.

Anti-positivism has been a response to the limitations of the abovementioned positivism and it says that the social world cannot be investigated in the same way as the natural world. Moreover, the position of anti-positivism is to reject empiricism and the scientific approach in social research and try to understand the interpreted experience of people of their situation. Anti-positivism consider that a phenomenon is both experienced and then interpreted using an individual's ideology, therefore, knowledge is something personally experienced and is not something that is acquired (Dash, 2005). Moreover, an anti-positivism approach sees the experienced situation as complex which can only be understood when all of the aspects of the situation are explored (Dash, 2005). Anti-positivism criticises the objectivity of science and prefers understanding subjectivity. The interviews in this study adopt an interpretative

approach because they aim to reveal the interpreted experience of the participants in relation to their relationship with the CSP and the concerns they may have.

4.2.2 Exploratory Approach

The study is based on a problem; that governments are reluctant to move to the next stage of cloud computing by placing sensitive in the public cloud and that a solution to this problem lies in the relationship that governments have with the cloud service provider. Therefore, there is an identified problem but the reasons for this problem which is the reluctance or lack of confidence of government is not fully understood. Therefore, it was found to be appropriate to adopt an exploratory approach to look for new insights into the problem and to generate ideas as part of the overall recommendations that the study will offer.

4.2.3 Qualitative Research

Within qualitative research there are a number of different approaches that exist which include to understand, to describe and to interpret phenomena experienced by individuals (Holloway and Wheeler, 2013). This study is concerned with trying to understand the phenomena of the relationship between the government and the CSP and the associated cloud factors of the public cloud, and therefore, adopts an exploratory approach. Moreover, qualitative research is used to help researchers explore the behavior and feelings of people (Holloway and Wheeler, 2013).

Qualitative interviewing has become increasingly popular in the social sciences and it is important to justify this approach in relation to the aims and objectives of the study (King and Horrocks, 2010). According to Tracy (2012) qualitative research is about being immersed in a scene and then trying to make sense of it. Importantly for the present study qualitative research is about understanding the ways that people see their world (Merriam, 2009) and this study is concerned with revealing issues related to the relationship between the government and the CSP and associated cloud factors. Therefore, a qualitative method, in this case, semi-structured interviews is adopted for this purpose.

4.2.4 Quantitative Research

Quantitative analysis involves data in the form of numbers and employs mathematical approaches to investigate their properties, referred to as statistical analysis which is designed to measure, make comparisons, examine relationships, test hypotheses, explore and explain (Walliman, 2011). Quantitative data can result from different research strategies and may

range from simple counts which could include the frequency of occurrences or more complex data which include test scores or prices (Saunders et al., 2016). Quantitative data by itself has little meaning and has to be analysed in order to derive meaningful information, this can be achieved through quantitative analysis techniques such as tables or diagrams which illustrate frequency of occurrence and statistical analysis that allow comparisons to be made through establishing relationships (Saunders et al., 2016).

The study uses a questionnaire to collect quantitative data about relationship and cloud factors towards answering the research questions which include to reveal issues about relationship factors and cloud factors and if there are certain cloud related factors that are affected by relationship factors, this is towards understanding the issues that may affect confidence in the public cloud.

4.2.5 Mixed Methods Research

Mixed methods research involves using both quantitative and qualitative data in a single study, which can allow complex phenomena to be examined in detail (Hickman, 2015). Using mixed methods is a way of capitalising on the strengths of qualitative and quantitative research while at the same time compensating for their limitations (Hickman, 2015).

This study will use questionnaires and although they can be a valuable method, they are more valuable when used in tandem with other methods, this is because one method is often not adequate (Gillham, 2008).

It is important to have a valid reason for the adoption of a mixed-methods approach and this relates to the appropriateness of this approach in answering the research questions of the research and the additional value that it offers (Hickman, 2015). The main research question of the study relates to revealing an understanding of relationship factors and associated cloud factors. There has been much written about the reasons that governments are reluctant which include factors such as trust and risk perception in relation to the CSP and the service they offer and cloud-specific factors such as security and privacy, governance and compliance, although these issues are known, the study will find out how these issues manifest in the relationship. This is based on the idea that the solutions to improving government confidence in the public cloud include technological solutions (improving security through technology) and improving the relationship, this study is concerned with contributing to the latter. Therefore, this study is concerned with these factors within the relationship between the

government as a customer and the CSP when they negotiate in the relationship. Using a questionnaire allows these known factors, derived from the literature, to be measured to further understand the relationship.

However, assumptions should not be made that the factors derived from the literature are the only factors that exist. In order to reveal new perspectives and concerns about the relationship and associated cloud concerns it is necessary to also employ a semi-structured interview. A semi-structured interview can provide a more detailed understanding of the issue. To provide an example that is related to the present study; a questionnaire may reveal that there are low levels of trust among government officials in relation to governance, or that government officials perceive a risk in relation to the management of data, and a semi-structured interview could reveal the reasons why there are these low levels of trust or high risk perceptions. The reason behind this approach is to achieve complementarity where the results of one of the methods can clarify or elaborate on the results of the other method, moreover, where quantitative processes provide the outcomes; the qualitative results reveal the processes behind the outcomes (Hickman, 2015). Adding a qualitative component here by investigating the experiences and perspectives of those individuals responsible for decision making will add a significant insight to the study (Hickman, 2015).

However, the knowledge we know, and the knowledge we don't is not the only justification for a questionnaire. Because we need to examine associations between cloud and relationship CSFs the questionnaire is the only way to do this because there are multiple variables and numerous combinations of those variables, and the only way to examine the relationship between them is with a questionnaire.

4.2.6 Reliability and Validity

In reference to reliability and validity they are important considerations for the development of the methodology and the analysis of the data. It is important that results are generalisable to the real world beyond the experiment itself. In order to achieve this there is a need for internal validity where independent variables are determined for the effect they have on the dependent variables, the external validity refers to the extent to which findings are generalisable (Walliman, 2011). In order to determine validity and reliability the data is inputted into SPSS and then checked using Cronbach's Alpha.

4.2.7 Credibility

Credibility is about how adequate or credible the social world under investigation is presented. One way of ensuring the validity is to check with the respondents. Groenwald (2004) suggests giving participants a copy of the questionnaire or interview transcript to validate them, this was achieved through a pilot study for both the questionnaire and the interview. Moreover, the researcher has to ensure that the methodology is credible, including data collection methods and interpretation of results (Lincoln and Guba, 1985).

4.2.8 Transferability

Transferability refers to how the researcher's working hypothesis can be used in other contexts (Lincoln and Guba, 1985). The researcher has to make sure that the data and its description is rich enough in order for other researchers to be able determine if the findings are transferable to other contexts.

4.3 Methods

4.3.1 Introduction

Here the adopted methods to achieve the aims and objectives and answer the research questions are presented. There is an explanation of why and how they are adopted for the study, specifically in relation to gaining qualitative and quantitative data. There is an explanation of how they are developed based on secondary research about relationship and cloud factors that are relevant to the government – CSP relationship.

The mixed methods design that is used in this study is a 'convergent parallel' design, this involves using qualitative and quantitative data concurrently to gain different but complementary data in order to answer the research question (Hickman, 2015).

Therefore, in reference to how qualitative and quantitative aspects are mixed, this study uses the 'integration' procedure suggested by Zhang and Creswell (2013) which means quantitative and qualitative data are collected concurrently but then analysed separately and the results are integrated during the interpretation stage.

4.3.2 Questionnaires

The term questionnaire is used to refer to all techniques where data is collected whereby a person is asked to respond to preset questions in a predetermined order and is one of the most

widely used data collection techniques used in the survey strategy (Saunders et al., 2007). It is important that the questionnaire is designed in a way that will allow the researcher to answer the research questions and achieve the study's objectives (Saunders et al., 2007).

In the present study, the questionnaires are based on knowledge that is already known about governments, their reluctance to adopt the public cloud and the associated reasons why, which are related to trust and risk perception and other relationship concerns and cloud specific concerns such as governance, compliance, security and privacy and performance.

The use of questionnaires in this study is appropriate to answer the following research questions:

1. What are the relationship and cloud factors that may affect the confidence of the Saudi government to adopt the public cloud?

2. Do relationship related factors and cloud factors affect each other which affects government confidence in the public cloud?

4.3.2.1 Justification for using questionnaire

The variables that are found within the relationship are already known, there are known issues of trust and risk perception related to government adoption of the cloud, and there are known cloud-specific issues such as governance, compliance and security. A questionnaire is suitable to reveal the level of opinion in terms of agreement related to these known factors within the context of the relationship. According to Gillham (2008) the researcher determines the questions and predetermines the possible answers, but the real intention is to find out which answers are selected. In other words, the researcher knows that there may be issues, for example, of trust and risk as relationship factors in relation to security and privacy as cloud factors, and the questionnaire will reveal if there are issues in these areas and to what extent.

Because the study is concerned with a number of relationship variables and cloud-related variables, in addition to the numerous variables that arise from the various combinations between the two, it would only be possible to address all of them using a questionnaire. Additionally, the responses to these numerous variables have to be analysed and a questionnaire using closed questions on a Likert scale will provide the type of data that is easier to analyse.

As an example, the questions in the questionnaire will address risk perception and trust in the relationship with the CSP and risk perception and trust in relation to requirements from the cloud. Together these form the critical success factors (CSFs), both relationship CSFs and cloud CSFs, success factors in that they would give confidence to governments as potential customers of the public cloud. This approach will reveal not only whether governments do not have confidence in the relationship with the CSP but also the specific areas or CSFs for cloud computing where there may be issues.

4.3.2.2 Sampling

There were four organisations that were identified for the study and each of these organisations had a limited number of personnel both senior and technical who are involved in the decision-making process either as those directly responsible for making decisions and those that influence decisions, all of which having a relationship with the CSP in some way. Because these organisations were government organisations and there were significant security considerations, given that the study is researching the issue of government in the cloud, the researcher had to liaise with a senior manager in each organisation to identify and have access to potential respondents.

Importantly, the criteria for selecting respondents for the questionnaire was that they were senior personnel who were involved in decision making about the cloud and have a relationship with the CSP, or that they were technical personnel who were involved in or who had influence over the decision-making process and have experience in dealing with the CSP. Because respondents to the questionnaire are selected according to these criteria in order to answer the research questions of the study, a non-probability sampling approach is adopted, specifically purposive sampling. Purposive sampling is selecting participants in a study based on their experiences or expertise that is a requirement in order to answer the research questions where there is a need for particular characteristics that are relevant to the theoretical concerns of the study (Howitt and Cramer, 2011). Purposive sampling is used when the respondents are selected with a specific purpose in mind and are specialists in a particular area (Neuman, 2014) again, in this study that specific purpose is to reveal the concerns found in the government – CSP relationship that could impede public cloud adoption. Moreover, it is inappropriate to use purposive sampling where there is a need to have a representative sample (Neuman, 2014), something that was not possible in this study due to the specialized nature of participants and the narrow criteria for selection. Therefore, there is a need for a

sampling strategy that is suitable for selecting unique participants that are particularly informative in terms of the research questions under investigation (Neuman, 2014), specifically here, those who can inform about decisions to adopt the cloud. A further reason for using purposive sampling, in addition to selecting specialised participants, is to reach groups that are difficult to reach (Neuman, 2014).

The point made in the above about identifying difficult to reach groups is relevant to the approach that the researcher of this study used to identify potential participants. To locate people who are specialists and decision makers and fit the criteria of this study the researcher had to use a certain amount of local knowledge and experts of where such people are located (Neuman, 2014). In this study, the researcher uses senior personnel in each of the four identified government organisations to identify suitable personnel according to the study criteria. It would not have been possible for the researcher to identify these personnel because of two main reasons, firstly; the researcher does not have inside knowledge of these organisations in terms of personnel and what they do, and secondly; because these are major government organisations in Saudi Arabia there are security considerations, the researcher cannot simply access these organisations and the personnel without the authority knowing who will be interviewed.

In reference to the size of the sample it is important to note that a sample of at least 30 is required if the researchers wants to carry out any type of statistical analysis, however, this may be considered a minimum number and it is recommended that there are more in the sample (Cohen et al., 2013). In studies that adopt non-probability sampling sample size is an ambiguous issue, this is because it is more important that the selection of the sample relates to the purpose of the study (Saunders et al., 2016), and because the study adopts purposive sampling, the sample size is not as important as selecting respondents based on the criteria that they are directly involved in or have influence over government decisions to adopt the public cloud.

One of the statistical analyses used in this study is correlation analysis using Spearman's correlation coefficient, and in reference to sample sizes using this technique it was found that the median sample size from five journal articles, between 2006 and 2010, varied between 73 and 178 (Fraley and Vazire, 2014)

A total of 95 respondents were identified from all of the four government organisations which included Saudi Customs, Immigration Department, Ministry of Finance and the National

Information Centre. All of these 95 potential respondents were given the questionnaire via email, this was administrated through the liaise in each organisation. In total, there were 80 responses and 15 did not respond.

4.4 Development of the Questionnaire

In chapter three the relationship factors that are critical to the success of the relationship between government and the cloud service provider, and therefore, critical to ensure confidence in the public cloud, were established. Moreover, towards achieving the aim of determining the specific areas of the cloud within the relationship the cloud critical success factors and cloud sub critical success factors were also established in chapter three.

These factors form part of the research enquiry and are therefore, included in the questionnaire towards achieving the aims of the study and answering the research questions. The following is a sample of the questionnaire to illustrate this structure.

Example of question structure:

Relationship CSF: ability to specify requirements (negotiation)

Main question: You are able to specify your requirements in relation to the following:

Cloud CSF: Governance

Sub Cloud CSFs:

- Knowledge and control over data, processes and applications
- Surety of other cloud tenants
- Knowledge and control over third party (CP) issues
- Clarity of roles and responsibilities / accountability (government and CSP)
- Dynamic SLA (towards mitigating risks, adapting to changing requirements)
- Control and knowledge of CSP employees
- Auditing and measuring of CSP
- Collaboration
- Governance during migration to the cloud

Based on the question structure described above, below (Table 4.1) is an example of a question in the questionnaire, note that the question is associated with the relationship factor

of risk perception in relation to the cloud related factor of governance and the associated factors within governance.

Sample question:

You can effectively specify your requirements in relation to the following: (Negotiation)

Table 4-1: Questionnaire question example

Question	1- Strongly disagree 2- Disagree 3- Neutral 4- Agree 5- Strongly Agree	1	2	3	4	5
NEGOTIATION DOMAIN						
Q5	You can effectively specify your requirements					
GOVERNANCE		**1**	**2**	**3**	**4**	**5**
Q6A	You can effectively specify your governance requirements					
Q6A 1-8	**You feel can effectively specify your governance requirements in relation to the following:**					
Q6A 1	Your need to have knowledge and control over data and processes					
Q6A 2	Assurance about other cloud tenants					
Q6A 3	Knowledge and control over third party issues					
Q6A 4	Clarity of roles and responsibilities					
Q6A 5	Dynamic SLA					
Q6A 6	Control and knowledge of CSP employees					
Q6A 7	Auditing and measuring of CSP					
Q6A 8	Governance during migration					
COMPLIANCE		**1**	**2**	**3**	**4**	**5**

Q6B	In the relationship with the CSP you are able to specify compliance requirements					
Q6B 1-8	**You can effectively specify your compliance requirements in relation to the following:**					
Q6B 1	Continuous auditing and assessment					
Q6B 2	Clarity and confidence about jurisdiction					
Q6B 3	Data management					
Q6B 4	Roles and responsibilities for compliance					
Q6B 5	Security and privacy					
Q6B 6	CSP ability to be compliant					
Q6B 7	Data location					
Q6B 8	Compliance when migrating					
SECURITY AND PRIVACY		**1**	**2**	**3**	**4**	**5**
Q6C	In the relationship with the CSP you are able to specify security and privacy requirements					
Q6C 1-7	**You can effectively specify your security and privacy requirements in relation to the following:**					
Q6C 1	Security related to third parties					
Q6C 2	Monitoring of policy adherence					
Q6C 3	Sufficient involvement in security					
Q6C 4	Tailored security and privacy policy					
Q6C 5	General security / privacy provision					
Q6C 6	Clarity of roles and responsibilities					

Q6C 7	Assurance regarding CSP employees					
PERFORMANCE AND OFFERING		**1**	**2**	**3**	**4**	**5**
Q6D	In the relationship with the CSP you are able to specify performance and offering requirements					
Q6D 1-9	**You can effectively specify your performance and offering requirements in relation to the following:**					
Q6D 1	Customisable cloud environment					
Q6D 2	Dynamic / flexible SLA					
Q6D 3	Continues monitoring of performance					
Q6D 4	Meet government specific requirements					
Q6D 5	Additional specialised staff for government needs					
Q6D 6	Backup and recovery					
Q6D 7	Sufficient support lifecycle					
Q6D 8	Sufficient notice of disruption					
Q6D 9	End of relationship					

Drafting the questions is a key stage in questionnaire construction, and part of this process is to identify the key topics especially in terms of which questions come first and how they lead one to another (Gillham, 2008). In this study, the questions are organised according to the identified relationship and associated cloud factors and proceed starting with trust, then risk, followed by negotiation and then collaboration and finally reputation. Although it has been stated that questions about attitudes and opinions are difficult to write, questions should be at a simple level because if they are not they may not be suitable for a wide-ranging questionnaire (Gillham, 2008). In consideration of this, the questions in the questionnaire are written in a simple way, this is achieved through a tiered system, illustrated in the following

where the relationship factor ‘trust’ and the cloud factor ‘governance’ are highlighted (see Figure 4.1):

Figure 4-1: Questionnaire Structure

Q1	**You trust your CSP**
QUESTION 2A	**GOVERNANCE**
Q2A	In the relationship with the CSP you trust them in relation to governance
Q2A 1-8	You trust the CSP in relation to the following governance issues:
Q2A 1	Your need to have knowledge and control over data and processes
Q2A 2	Assurance about other cloud tenants
Q2A 3	Knowledge and control over third party issues
Q2A 4	Clarity of roles and responsibilities
Q2A 5	Dynamic SLA
Q2A 6	Control and knowledge of CSP employees
Q2A 7	Auditing and measuring of CSP
Q2A 8	Governance during migration

In order to achieve the aims of the study it is necessary to reveal people’s opinions based on their experiences of CSPs. The most common way of revealing these opinions in a questionnaire is to ask to respondents to rate their level of agreement or disagreement on a scale of five points (Smith et al. 2012). Some studies do employ a seven-point scale, however, it is more difficult to find descriptive terms for each point as they increase in number, and the five point scale is more commonly used, this is an odd number, and therefore, allows for a neutral response (Tullis and Albert, 2013). In this study 1 indicates strongly disagree, 2 disagree, 3 neutral, 4 agree and 5 strongly agree. Moreover, in this approach there is the assumption that the people that participate have attitudes towards the issues that are being investigated and that these attitudes can be reflected in the rating system (Smith et al., 2012). To ensure this, this study has chosen participants who have had dealings with cloud services providers and are influential in the decision-making process.

Specifically, in line with the aims and objectives of the study which include finding out the relationship factors that could affect the government’s confidence to place sensitive data in the public cloud, there is a need to examine concerns that are related to risk perception and trust within the context of a relationship. There are a number of relationship-based critical

success factors (CSFs) based on risk, trust, collaboration, negotiation and reputation that have been identified in the literature as well as cloud CSFs based on governance, compliance, security and performance as cloud factors, that are used to form the questions. Moreover, the literature has revealed that there are a number of different concerns that relate not only to government use of the cloud generally, but also to government use of the public cloud for sensitive data on a longer-term more permanent basis. These concerns are found within the cloud factors and are presented as sub cloud factors in this study.

4.4.1 Relationship Critical Success Factors

The literature has also shown that the reluctance, both of governments and other organisations, to use the public cloud is related to issues such as trust and risk perception and within these issues, for example, the ability to specify requirements and have requirements understood. These ideas are found in general theories of trust, risk perception and collaboration such as Protection Motivation Theory (PMT), Risk Compensation Theory and Collaboration Fluency, and theories of trust that are related to IT procurement (Rothstein, 2007). More specifically in relation to the study, there are numerous Cloud Trust Models that have been proposed to help organisations overcome trust concerns. Together these theories and models serve to inform issues when considering the reasons why governments are reluctant and have concerns about placing sensitive data in the public cloud. Therefore, a method that is designed to investigate the reasons related to such concerns should be based on ideas of trust, risk perception, collaboration, negotiation and perception of reputation.

The study aims to find out trust and risk related concerns within the relationship where government requirements for the cloud are negotiated. In order to discover relationship-specific issues and associated cloud-specific concerns it was first necessary to establish Critical Success Factors (CSFs) of an effective relationship as standards against which aspects of the relationship in this study can be investigated. These CSFs are derived from the literature. For example, a relationship CSF is that the CSP is able to understand the government's requirements and respondents will be questioned to find out the extent to which they feel this is true in relation to areas of the cloud. Furthermore, an associated sub cloud CSF could be governance over data and the questions are also designed to see if the participants have any issues about these factors in the relationship. These ideas are based on the premise, derived from the literature, that in a more successful relationship there would be the establishment of trust, a decrease in the perception of risk, effective negotiation, a

perceived positive reputation and collaboration which would include, for example, the ability to specify requirements and have those requirements understood and catered for. In this study success in these areas will form Critical Success Factors (CSFs) for an effective relationship and will be categorised under relationship factors that will be investigated using the questionnaire. In addition to these relationship CSFs there are the cloud CSFs themselves which include governance, compliance, security and privacy and performance and offering, and the sub Cloud CSFs in each of these areas. These CSFs form the basis of the questions in the questionnaire.

Figure 4.2 below shows the relationship CSFs, here it shows how the questions are structured in the questionnaire, the first box represents the relationship CSFs that are being addressed, the second box represents the cloud CSFs that are considered with the relationship CSFs, and the third box represents the sub cloud CSFs within each cloud factor. To provide an example, a question will be concerned with the issue of trust (relationship CSF) and will question to find out if there is an issue of trust in relation to the cloud CSF of governance and each of the associated sub factors such as process execution or control over data.

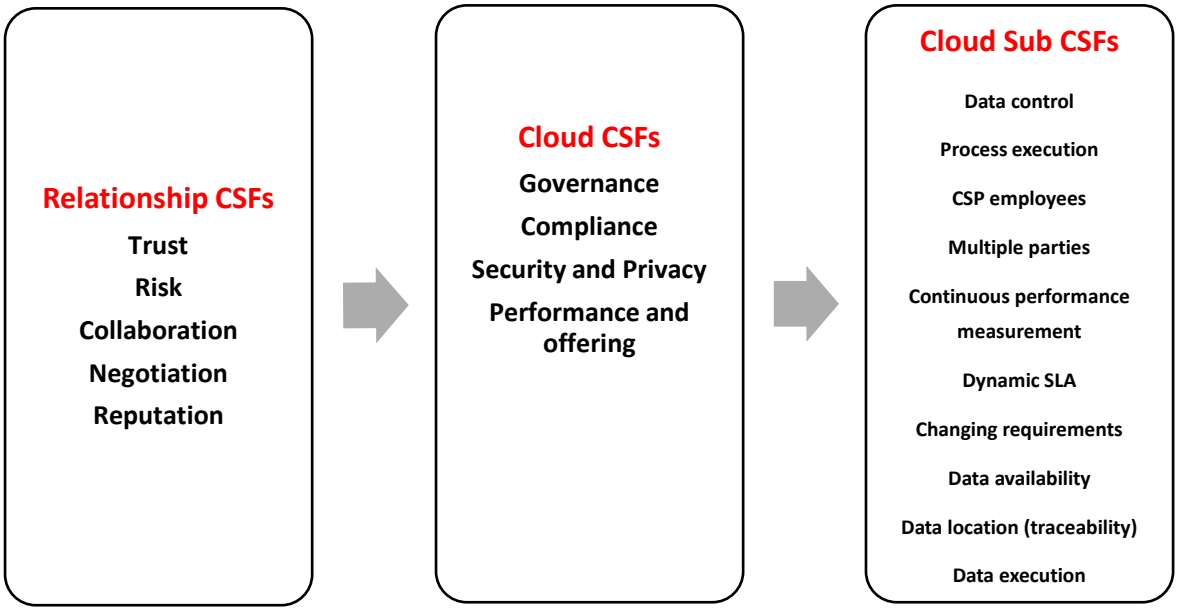


Figure 4-2: Critical Success Factors (CSFs) for Questionnaire Development

The relationship CSFs are derived from the literature about general theories of trust, risk and collaboration, IT trust models and theories and cloud trust models (see Table 4.2).

Table 4-2: Relationship Factors

	General Theories of Trust, Risk and Collaboration	IT Trust Models and Theories	Cloud Trust Models
Trust	Trust in what provider will do that is not in contract (Blomqvist et al. 2008). Sharing of information between parties (Blomqvist et al. 2008). Trust is required for better communication and collaboration (Grudinschi et al. 2014). Trust required for governance (Blomqvist et al. 2008). Trust can develop quickly if intense interaction and collaboration (Blomqvist et al. 2008). Relationship takes time to establish (Thomson et al. 2009).	Trust in ability. Trust in integrity. Trust in Benevolence. Trust in confidentiality (Firdhous et al. 2011). Control and transparency (Firdhous et al. 2011).	Two-way trust (Kanwal, 2015). Ongoing trust – measurement of performance (Kanwal, 2015, Filali and Yagoubi, 2015). Aligned interests (Jansen and Grance, 2011). Extent to which cloud service meets expectations (Burda and Teuteberg, 2014). Trust is goodwill, integrity and competence (Huang and Nicol, 2013).
Risk	Ability to mitigate risk (Protection Motivation Theory). Service provider alleviates perception of risk (Protection Motivation Theory).	Risk perception (privacy, security etc.). Extent of willing vulnerability (Burda	Third parties not bound by SLA (Alhamad et al. 2010). Flexible risk management program that adapts to constantly changing risk landscape (Jansen and Grance, 2011).
Collaboration	Trust = better communication and collaboration (Grudinschi et al., 2014). Clarity of roles and responsibilities (Thomson et al. 2009). Mechanism to measure parties activities in terms of roles and responsibilities (Thomson et al. 2009). Reciprocation (Thomson et al. 2009).	IT procurement and importance of collaboration in the public sector (Grudinschi et al. (2014).	Dynamic / flexible SLA (Di Modica, 2014, De La Prieta et al. 2015, Filali and Yagoubi, 2015). Continuous monitoring of SLA adherence (Alhamad et al. 2010, Marudhadevi et al. 2014). Informed how data/systems will be managed. Transparency of QOS for SLA adherence (Kanwal, 2015). Real time agreement (De La Prieta et al., 2015). Collaborative development of SLA (CSA Guidance).
Negotiation	Governance and ongoing process that requires continuous negotiation to create equilibrium (Thomson et al., 2009).	Express business needs (Johanssen and Latinen, 2012).	Ability to specify / articulate requirements (Di Modica, 2014, Alruwaili and Gulliver, 2014). Having requirements understood (Di Modica, 2014). Ability to negotiate each area of SLA (Di Modica, 2014). Resolution of conflicting objectives (Dastjerdi and Buyya 2015, Alhamad et al. 2010). Needs of customer are considered / offered (Di Modica, 2014).

Reputation	Reputation achieved through numerous interactions where trust is built (Thomson et al., 2009). Link between trust and reputation (Huang and Nicol, 2013).	Prior knowledge experience with CSP (Firdhous et al. 2011).	Reputation of CSP (Parwar et al. 2012, Norr et al., 2016). Sufficient information of CSP (Alruwaili and Gulliver, 2014).

The aforementioned relationship factors shown in Table (4.2) serve to inform the relationship CSFs found under the areas of trust, risk, collaboration, negotiation and reputation. It would be difficult to consider all of the factors in Table (4.2) in the questionnaire so they are summarised into relationship CSFs as shown in Table (4.3) below. These CSFs form the basis of the development of the questionnaire.

Table 4-3: Relationship Critical Success Factors (CSFS)

Trust in ability.
Trust in integrity.
Low perception of risk.
Ability to specify requirements.
Requirements are understood / considered by CSP.
Sufficient information about CSP.
Perception of positive reputation of CSP.
Communication / sharing information.
Dynamism and flexibility.
Transparency,
Continuous collaboration,

4.4.2 Cloud Critical Success Factors

To address the concerns of government in relation to the public cloud it is also necessary to consider the specific concerns that they have related to using the cloud itself. Although

governments do share common concerns with other organisations such as security and privacy, they have their own unique concerns due to the type of data that they handle and the need to be compliant with laws. Particular concerns for governments include governance, compliance, security and privacy and performance and offering. Here each of the areas of cloud CSFs identified in the literature are presented followed by a summarisation.

Table 4-4: Cloud Critical Success Factors (CSFs)-Governance

Cloud CSF	Cloud sub CSFs
Governance	Data control (Kanwal, 2015). Data execution (Brender and Markov, 2013). Data availability (Kanwal, 2015). Knowledge of data location (Brender and Markov, 2013, (CAIQ) (v3.0.1). Process execution (Kanwal, 2015). Remote access control (Firdhous et al 2011). Accessibility (Norr et al. 2016). Control over definition of access rights (Norr et al. 2016). Accountability over deployed applications and systems (Jansen and Grance, 2011). Control over transfer of data (Brender and Markov, 2013). Continuous access during all situations – normal and disaster (Kanwal, 2015). Clear ownership rights over data (Jansen and Grance, 2011). Knowledge of movement of data within the cloud (CSA Guidance). Knowledge of who has control over data (CSA Guidance). Collaborative governance structures (CSA Guidance). Knowledge and control over CSP employees (Brender and Markov, 2013, CSA Guidance). Control over other tenants in cloud (Jansen and Grance, 2011) (Access control) Takabi et al (cited in Alhamad et al 2010). Not share cloud resources with competitors (other tenants) (Almorsy, 2011). Clarity of roles and responsibilities (Jansen and Grance, 2011). Alignment of policies regarding assignment of roles (Jansen and Grance, 2011). Transparency of CSP actions (Firdhous et al 2011). Knowledge of third party relationships (Alhamad et al. 2010, Firdhous et al. 2011). Control over third parties (Takabi et al (cited in Alhamad et al 2010). Third party identity management (Takabi et al (cited in Alhamad et al 2010). Trust in supply chain (CSA Guidance). Policy integration with third parties (Takabi et al (cited in Alhamad et al 2010) (Jansen and Grance, 2011). Multiple distributed clouds used by CSP – trust relationship required between customer, CSP and CPs (Fan and Peros, 2014).

	Security requirements aligned between three parties (CP, CSP and customer) (Almorsy, 2011). Do CPs understand security requirements (Almorsy, 2011). Duality in trust (Kanwal, 2015). Dynamic SLA (Kanwal, 2015). Measuring other parties activities (Kans, 2012). Framework to monitor and measure risk (CSA Guidance). Clarity of who will have access to data (CSA Guidance). Mechanism for vetting those who have access to the data (CSA Guidance). Clarity of what activities for what type of information (CSA Guidance). Clarity of which users for which type of information (CSA Guidance). Control over security policy (Ahmad and Janczewski 2011). Direct point of contact in CSP (Jansen and Grance, 2011). Maintaining situation awareness (in order to weigh up options and set priorities) (Jansen and Grance, 2011). Ability to enforce control and maintain accountability (Jansen and Grance, 2011). Auditing mechanisms for data storage, protection and use (Jansen and Grance, 2011). Organisational practices (government) followed by CSP throughout system lifecycle. Adequate oversight to maintain accountability (Jansen and Grance, 2011). Control over deployed applications (Jansen and Grance, 2011). Sufficient recourse to address and resolve problems (Jansen and Grance, 2011). Sufficient risk mitigation through negotiated SLA (Jansen and Grance, 2011). Governance during migration to the cloud (Estonia Report).

Table 4-5: Summarised Critical Success Factors (CSFs) for Governance

Governance CSFs	**Description**
Knowledge and control over data, processes and applications.	Governance requires a certain level of control over data and processes, it is also an important consideration for compliance.
Surety of other cloud tenants.	Governance requires government has a level of control over other parties in the cloud.
Knowledge and control over third party (CP) issues.	Knowledge and control of the CP as a provider of the cloud to the CSP is required for governance.
Clarity of roles and responsibilities / accountability (government and CSP).	In order to maintain a level of governance it is necessary to know who is responsible for what, in both the government and the CSP.
Dynamic SLA (towards mitigating risks, adapting to changing requirements).	Governance is negotiated in the SLA.

Control and knowledge of CSP employees.	Governance is only possible is government know who the employees are and has the required level of control over employees.
Auditing and measuring of CSP.	Auditing, monitoring, measuring of CSP performance, activities and risk.
Collaboration.	Governance requires collaboration between government and CSP.
Governance during migration to the cloud.	Government need a level of involvement and control over migration to the cloud.

4.4.3 Combination of Relationship and cloud Critical Success Factors (CSFs)

In the above the relationship and cloud critical success factors have been identified and summarised. In the following the structure of the questionnaire, based on the identified CSFs, is explained. The starting point of the question is the relationship CSFs because the study aims to address the relationship, followed by the cloud CSFs as it is important to understand specific areas where there are concerns and an associated lack of confidence. For example, governments may feel that they cannot specify their governance requirements specifically in relation to the CSPs employees, but may be more confident in specifying governance requirements in relation to data control. In this regard, Table 4.6 illustrates the question structuring of the questionnaire.

Table 4-6: Questionnaire Structure

Relationship CSF	Main question	Cloud CSF	Sub Cloud CSFs
Understands requirements	**Your service provider understands your requirements in relation to the following:**	Governance	Data control Data execution Process execution CSP employees Multiple parties Continuous performance

			measurement Dynamic SLA Changing requirements Data availability Data location (traceability)

Based on the question structure described above, below (Figure 4.3) is an example of a question in the questionnaire, note that the question is associated with the relationship factor of risk perception in relation to the cloud related factor of governance and the associated sub factors within governance.

You perceive a risk in relation to the following:

Figure 4-3: Questionnaire question example

RISK DOMAIN 1. Strongly Disagree 2. Disagree 3. **Neutral** 4. Agree 5. Strongly Agree						
Q3	**In your relationship with the CSP you do not perceive a risk**					
QUESTION 4A GOVERNANCE						
Q4A	When engaging in the relationship with the CSP you do not perceive a risk in relation to governance					
Q4A 1-8	**In the relationship with the CSP you do not perceive a governance risk in relation to the following:**					
Q4A 1	Your need to have knowledge and control over data and processes					
Q4A 2	Assurance about other cloud tenants					
Q4A 3	Knowledge and control over third party issues					

Q4A 4	Clarity of roles and responsibilities					
Q4A 5	Dynamic SLA					
Q4A 6	Control and knowledge of CSP employees					
Q4A 7	Auditing and measuring of CSP					
Q4A 8	Governance during migration					

Now that the contents of the questions have been established how the questions should be asked needs to be addressed. In the above it was shown that the questionnaire is designed to find out about a number of relationship and cloud related factors.

Balanced scores are a way of measuring attitudes and they have to be balanced by using an equal balance of negative or positive statements (Brace, 2008). The most commonly used number of points on this scale is five. The questions are presented as level of agreement on a Likert scale with two levels of agreement, two levels of disagreement and a neutral response which represents neither agree or disagree.

4.4.4 Analysis of Questionnaire Data

The data gained from the questionnaires was analysed using SPSS (Statistical Package for the Social Sciences) in order to answer the research questions. Analysis was carried out to find relationships in the data between relationship factors and cloud factors. Specifically, correlation analysis was conducted using Spearman's correlation two-tailed significance in order to find correlations between the established variables towards achieving the aims of the study. Spearman's rank order correlation is a non-parametric method of statistical analysis that measures the strength of association or statistical dependence between two ranked variables.

4.4.5 Piloting of the Questionnaire

In order to ensure the validity of the questionnaire, in other words to determine if the questionnaire is measuring what it is supposed to be measuring, it is necessary to pilot the questionnaire (Brace, 2008). Moreover, ensuring the reliability of the questionnaire requires

that the questions are checked for understanding by the participants and that they produce meaningful responses (Brace, 2008).

Specifically, in order to test for reliability, the researcher checked with departmental management if the questions sounded clear and understandable. Moreover, the questions were also check to see if they contained any jargon (Brace, 2008). It is important to note that the questions in the questionnaire contain a lot of information about the cloud, including technical aspects, and this information is only familiar to those who are involved in the cloud from a technical perspective. Therefore, there may be some ideas and even jargon that needed to be verified for clarity of understanding.

Another important aspect of a questionnaire that affects its reliability is the procedure or routing instructions of the questionnaire (Brace, 2008). In this study, the respondents to the questionnaire have to answer general relationship questions followed by associated cloud and sub cloud questions, all of which still contain a relationship element. Therefore, part of the piloting was to test not only if they understood the questions but if they understood that they were being asked about cloud and relationship factors at the same time.

Specifically, to ensure validity those who participated in the pilot were checked to see if they could answer the questions properly, this was achieved through explaining the Likert scale responses. The piloting took place with five participants from the Saudi Customs and no problems were identified.

4.5 Interview

In reference to the mixed methodology approach discussed in the above, the questionnaires measured relationship and associated cloud concerns using predetermined factors, however, a weakness of the questionnaire is that it does not reveal new factors as new knowledge. Therefore, as part of the mixed methods approach, a semi-structured interview is adopted for this purpose. In order to answer the research questions, it is necessary to interview those responsible for making decisions about the adoption of public cloud and the possibility of deploying sensitive data, this also includes personnel who influence the decision to adopt the cloud due to their technical expertise in this area. In order to achieve this, the study conducts semi-structured interviews with senior management and senior technical personnel to reveal

the relationship reasons behind reluctance of using public clouds and the specific cloud factors that are affected.

It is important to note that the main purpose of interviewing is not necessarily about testing a hypothesis or making an evaluation, but it is more about understanding the lived experience of other people and the meaning behind that experience (Seidman, 2013) something this study aims to do. In light of this it was felt that interviews were appropriate to understand the perception of senior decision makers in the relationship they have with cloud providers and the associated concerns.

4.5.1 Semi-structured

In qualitative research, different types of interviews can be used, these include semi-structured and unstructured interviews. Semi-structured interviews were used in order to derive insights into the reasons why choices are made and what influences decisions. A semi-structured interview is designed to obtain descriptions of the life world of the interviewee in order to interpret the meaning of a particular phenomenon (Kvale and Brinkmann, 2009).

The researcher did not want to have a formal and full interview with a structure because it may make the interviewee feel uneasy but the researcher did want to have an informal chat either because there were specific areas that needed to be discussed. There was a need for some structure while at the same time being open in style (Gillham, 2000) thus the semi-structured interview was adopted. In qualitative interviewing, there is focus on the opinion of the interviewee and they are encouraged to ramble or speak freely because it provides a deeper insight into what they see as important and relevant (Gillham, 2000).

Because the issue that is being researched requires an in-depth exploration of the relevant issues and there may be a need to encourage interviewees to talk more deeply about something they have raised, there may be a need to use probing questions in order for interviewees to clarify and extend their responses which interviews are suitable for (Gillham, 2000).

4.5.2 Development of the Semi-Structured Interview

The semi-structured interviews are designed to investigate the relationship between government and cloud service provider in order to determine the reasons why governments are reluctant to adopt the cloud. As with the questionnaire the primary focus is on the

relationship factors in the negotiation, however, the questions will also try to find out the cloud related factors that are of concern to governments when considering the public cloud.

In the development of the interview it is first important to focus on the research questions in order to decide what specific questions can be asked and can these questions be answered by talking to people (Gillham, 2000). Importantly, the questions are designed to allow the participant to speak freely about the topic being questioned, for example the question '*Do you trust your CSP?*' is not intended as a closed question where the participant will simply say 'yes' or 'no', it is the responsibility of the interviewer to probe further into the answers to each question, in this case the interviewer will ask why they trust or not trust their CSP.

In a semi-structured interview the researcher will have a list of questions and themes to be covered (Saunders et al., 2007). In this study, the themes which include trust, risk, negotiation, collaboration and reputation, which have also been identified for the questionnaires, are found within relatively simple and understandable questions which can be elaborated on in the answers. The interview questions are as follows:

1. *Do you currently have plans to use the public cloud for sensitive data and critical systems?*
2. *What are the concerns that you have about the public cloud?*
3. *How is your relationship with your CSP?*
4. *Do you trust your CSP?*
5. *In relation to your CSP, do you perceive any risks?*
6. *Are you able to negotiate effectively with your CSP?*
7. *Do you feel that concerns can be resolved through the relationship with the CSP?*
8. *Does your CSP accommodate all your needs?*
9. *Are you kept informed by your CSP?*
10. *How do you collaborate with your CSP?*
11. *How involved are you with the provision of the public cloud as a service?*
12. *Do you perceive a positive reputation of your CSP?*

It is important to note that there is certain amount of flexibility in a semi-structured interview, so the above questions do not have to be strictly adhered to, depending on the responses of the participant the researcher may adjust questions to probe deeper into certain issues, or they

may include other questions that prevent the participant from straying away from the research topics.

4.5.3 Conducting Interviews

Arrangements for the interviews are made with each of the participants individually. Because of the senior status of the participants and the nature of the job of the researcher permission was not required to use available offices on the premises; this was case for all four organisations. The researcher is a trainer in Saudi Customs department and could also facilitate a room without permission.

It is important in Saudi culture that when interviewing a participant that their immediate superior manager is informed, some of the participants in this study are senior officials and it requires informing the ministers themselves.

It was important that the interview was conducted in a room where there are no interruptions, no background noise and no curious intrusions (Gillham, 2000). The interviews lasted between one to one and a half hours, this was to allow for flexibility in terms of allowing for respondents who may want to elaborate of their responses or to allow the researcher to probe further based on responses.

The interviews were be audio recorded and conducted in English. It is important to ensure that the participants' words are preserved as accurately as possible and the best way to ensure this is through audio recording, moreover, this also records the questioning as well (Holloway and Wheeler, 2013) so that the researcher can check the responses against the questions for further clarity.

4.5.4 Analysis of Interview Data

It is difficult to separate the data collection from the data analysis because even when the researcher is collecting the data, in the case of the present study conducting the interviews, the researcher may anticipate results based on what they have already heard (Seidman, 2013).

Seidman (2013) says that in order to analyse the words that are spoken properly it is better to transform them into a written text through transcription, moreover, it is important that words are transcribed directly so that interpretation by the researcher is minimised.

The researcher analyses the data looking for emerging themes or substantive statements and then organising those ideas. Not only is it important to derive themes but it is also important to organise them in a way that shows how they are conceptualised and how they are related to each other, they will also involve a hierarchical representation which will include sub-themes (King and Horrocks, 2010).

Although there are two main approaches to analysing the interview transcripts, namely; meaning and content analysis (Kvale, 2008), it is possible that interview analysis is conducted without following a specific analytical method, that the researcher can switch freely between different techniques (Kvale, 2008). In light of this it was decide to adopt this approach, for example to derive meaning from the transcripts through coding and categorising through attaching key words to a segment of text.

4.5.4.1 Coding

Coding is about marking different sections of the data by using labels and proceeds towards the categorisation of data into themes (Holloway and Wheeler, 2013). The researcher reads through the transcript and identifies what they feel is important to both the researcher and the participant. During this initial coding, the researcher identifies words or phrases that the participant use in order to discern important ideas that are found within the data (Holloway and Wheeler, 2013). The method that is adopted is manual coding.

4.5.5 Piloting of Interview

Piloting of the semi-structured interview was carried out in order to check for clarity in the question and to find out if the questions elicited long or elaborate answers, in other words, did the design of the questions encourage the respondents to speak freely and in depth about areas that the researcher is interested in.

Like with questions in the questionnaire the order in which questions are asked and the links between them are important, and also like with a questionnaire the interview schedule has to be piloted and refined (Smith et al., 2012).

A small sample of three people from the same population of those who are to be interviewed was taken for the interview piloting. The pilot test was then checked for ambiguous sounding questions, questions that lack relevance and questions that contain jargon or advanced

vocabulary (Smith et al., 2012). Overall, the participants were satisfied with the clarity of the questions.

4.5.6 Sampling

The study requires that those who will take part in the interviews will have both knowledge of the subject and influence over the government decision making process or direct involvement. From the chosen organisations are personnel who are responsible for strategy formulation and implementation of cloud technology for the government. Therefore, it was decided to adopt purposive sampling because it is a form of sampling where there is no attempt to create a sample that statistically represents a certain a population but instead chooses people 'with purpose' that will allow the researcher to explore their research questions (Matthews and Ross, 2010 p.167). These participants in the research are chosen based on experiences that are related to the topic that is being researched, so that they can reveal much about the research area (Matthews and Ross, 2010).

Purposive sampling was adopted because it is a form of non-probability sampling where individuals are included in the study because they fit certain criteria because, for example, they have the specialist skills or knowledge that is relevant to the research (Jupp, 2006). There are some types of type of research that require the researcher to decide about which types of participants are likely to contribute relevant data. Therefore, the study adopts purposive sampling which is to choose the participants that are relevant to the study and its aims and objectives.

For the present study participants were chosen because of their specialist knowledge of information systems in their respective departments and ministries and because they are involved in the decision and deployment of government services to the cloud and have significant influence in this process.

For the semi-structured interviews the sample will include those senior government officials and technical staff who are directly involved in, or influence the decision of whether or not to adopt the public cloud for sensitive data. Specifically, in the present study there will be senior personnel from the Ministry of Finance Saudi Arabia, Saudi Customs which is under the Ministry of Finance, the Saudi Immigration Department and the National Information Centre, both under the Ministry of Interior. In total, there are 12 participants in the interviews, three from each of the aforementioned organisations. Those interviewed are in senior positions in

ministries and government agencies in Saudi Arabia and are directly responsible for decision making. For research that involves a homogenous group, 12 interviews are enough (Saunders et al., 2016). The participants in this study are homogenous because they are government cloud experts.

4.5.7 Access

Before the participants were selected for the study the researcher had to gain access to them. Due to the nature of the researcher's job he is well acquainted with senior officials in the four organisations. These acquaintances hold senior positions in IT and were deemed to be suitable for this study because of their decision-making powers. Moreover, these senior officials were able to introduce the researcher to other senior officials who are also involved in decisions about IT and cloud deployment, helping the researcher to identify 12 participants in total.

4.5.8 Ethical Considerations for Interviews

Ethical issues may arise using interviews due to the complexities of researching something that may be private and then opening those accounts to the public (Kvale, 2008). Ethical issues have to be considered throughout the entire interview research from the beginning to the final report (Kvale, 2008).

An important ethical issue is the informed consent to participate in the study and participant confidentiality (Kvale, 2008). In light of this the participants in the study were provided with two documents. The first document is an information sheet about the purposes of the study and the rights of the participants in terms of their right to confidentiality, data privacy and protection and their right to leave the study at any time. The second document is an informed consent form whereby potential participants give signed consent to participate in the study. Confidentiality in the present research is assured and any identifying data of the participants will not be reported (Kvale, 2008). The participants were told about the nature of the study and about their rights to leave the study at any time, moreover, they were informed that the study will be anonymous and their data will be kept in a secure location.

People are vulnerable to the apparent interest of an interviewer and because of this the interviewee may disclose extraordinary information, and the relationship between interviewer and interviewee is impersonal which seems to facilitate disclosure (Gillham, 2007). Therefore, because participants may be willing to speak more freely, it is important to respect

their anonymity and not disclose what any individual has said about their organisation and the issue being investigated.

4.6 Summary

This chapter presented the methodological considerations, including the research philosophy, for the study. Moreover, the approach to the research and the adopted methods were described and justified. The chapter also include an in-depth description of the development of the research methods. Finally, there was consideration of analysis techniques and ethical considerations.

5 Results and Analysis - Questionnaires

Objectives

- **Present the findings for the questionnaire**
- **Findings for relationship, cloud and sub cloud factors**
- **Analysis of findings**

5.1 Introduction

The results of the questionnaires are presented in this chapter which include the relationship, cloud and sub cloud factors and the connections between them. These factors are analysed in order to reveal the issues in the relationship towards achieving the aims and objectives and answering research questions of the study. The analysis considers both the cloud factors and the relationship factors and the interplay between them towards understanding the reasons for the reluctance to adopt the public cloud by government. Specifically, cloud and sub cloud factors are analysed against the relationship factors in order to show where in the relationship between the government and the CSP the issues about the public cloud are. Moreover, towards further understanding the relationship, analysis is conducted between relationship factors to see if there are links between them, and this is conducted in relation to all cloud and sub cloud factors. The reason for this analysis is to see if relationship factors have different implications for different cloud and sub cloud factors.

5.2 Reliability Statistics

Cronbach's Alpha is a mathematical method for calculating reliability and is used for assessing the reliability of the variables, namely, the relationship, cloud and sub cloud factors. The initial part of the reliability analysis, showed in Table 5.1 indicated that the Cronbach's Alpha was 0.988 for 333 items.

Reliability was established for all variables, namely, the relationship, cloud and sub cloud factors in the questionnaire. This was achieved through employing internal consistency with Cronbach's Alpha. The calculated Cronbach's Alpha for each factor is presented below in Table 5.1. The results show that all of the relationship factors received a high level of reliability. Factors with Alpha coefficient values of greater than 0.7 are considered to be reliable, here the values range from 0.875 to 0.988, therefore, the factors are internally reliable.

Table 5-1: Reliability Statistics

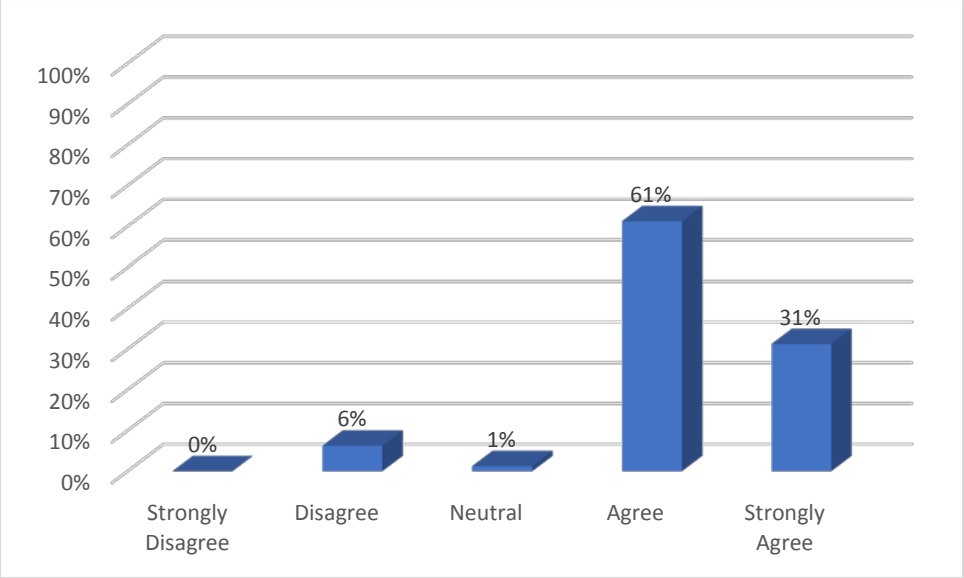
	Reliability Statistics		
No	**DOMAIN**	**Cronbach's Alpha**	**N of Items**
1	TRUST DOMAIN	0.918	37
2	RISK DOMAIN	0.875	37
3	NEGOTIATION – specify requirements	0.912	37
4	NEGOTIATION – CSP understand requirements	0.919	37
5	NEGOTIATION – ability to negotiate	0.94	37
6	COLLABORATION – effectively collaborate	0.916	37
7	COLLABORATE – effectively communicate	0.919	37
8	REPUTATION – sufficient information	0.894	37
9	REPUTATION – perceive positive reputation	0.918	37
10	**OVERALL RELIABILITY**	0.988	333

5.3 Trust Domain – Relationship Factor

This chapter is organised according to the relationship factors and considers frequencies, correlation with cloud factors and sub cloud factors, and correlation with other relationship factors in relation to cloud factors.

The results show that in response to the statement ‘you trust your CSP’ the vast majority of respondents, 92 percent agreed with this idea, with 31 percent strongly agreeing (see Figure 5-1). Only 6 percent disagreed with this idea. Therefore, there is an overall high level of trust in the CSP where trust is considered generally without consideration of cloud factors or other relationship factors.

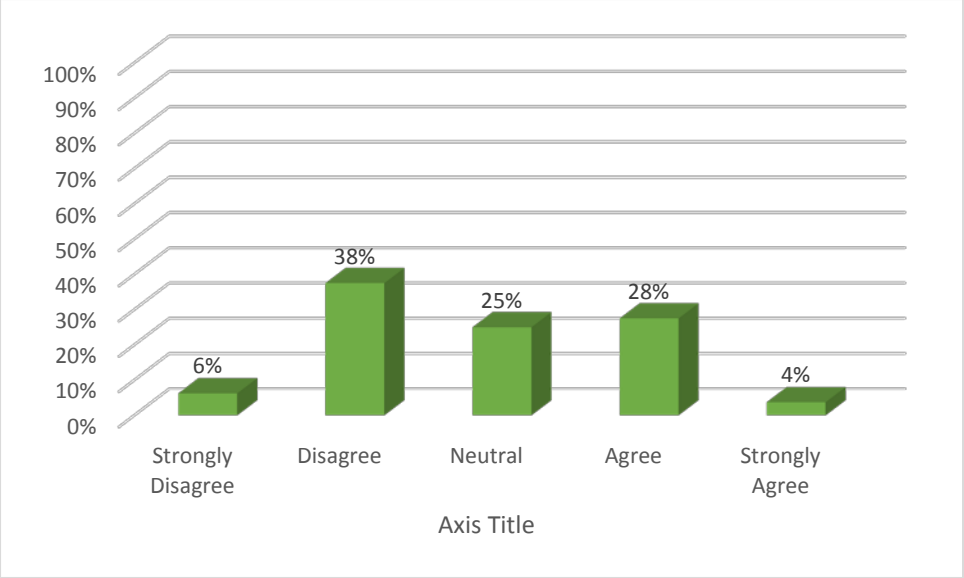
Figure 5-1: You Trust Your Cloud Service Provider (CSP)



5.3.1 Trust and Governance

Trust is analysed against the various cloud factors and associated sub cloud factors in order to show the interplay between relationship and cloud factors. In reference to trust in governance generally, there were a significant number of respondents, 25 percent, who gave a neutral response to the statement that they trust their service provider. The majority of the respondents, 44 percent, disagreed with the idea that they trust their CSP. However, a significant number, 28 percent agreed and 4 percent strongly agreed that they trust the CSP in relation to governance. In comparison to trust generally, when respondents were asked about trust in relation to a cloud factor specifically, in this case governance, there was a significant decrease in the level of trust. This shows that for consideration of governance as a specific cloud factor here shows less trust in the CSP (see Figure 5-2). However, it has to be noted that a quarter of the respondents gave a neutral response, which indicates a level of uncertainty for governance.

Figure 5-2: Trust Cloud Service Provider (CSP) in Relation to Governance



5.3.1.1 Trust and Sub Cloud Factors of Governance

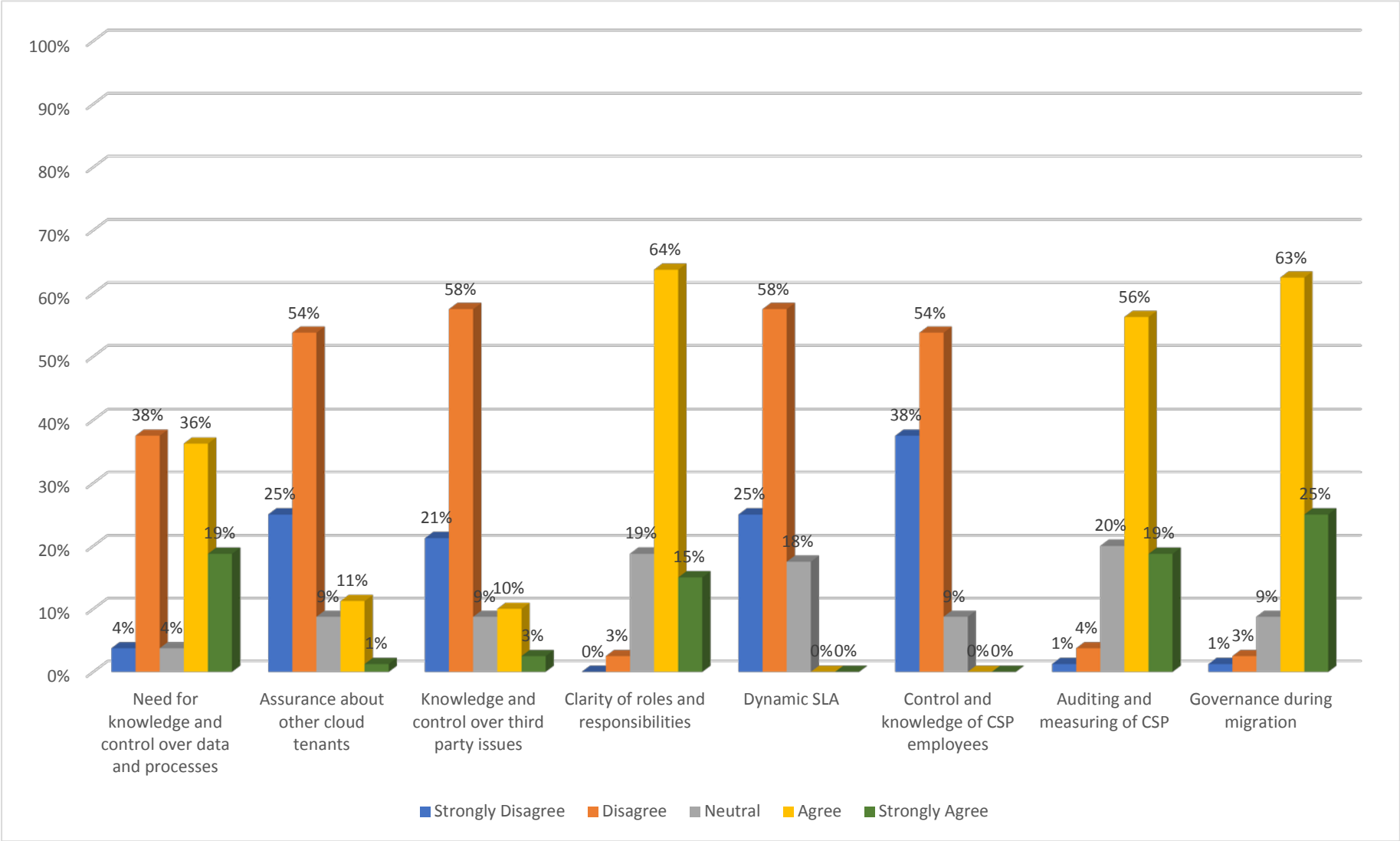
For the sub cloud factors of governance, the government trusted the CSP the least in relation to *Control and knowledge of CSP employees*, this was followed equally by *Dynamic SLA* and *Assurance about other cloud tenants*, there was also mistrust of *Knowledge and control over third party issues*. These are issues that are pertinent to government in consideration of the cloud and governance over data and systems. Governments have a specific duty to protect data and that would include knowing about who is employed by the CSP and potentially has access to government data, or at the least be assured by the CSP about their employees. In regard to the dynamic SLA one of the reasons for government being reluctant to adopt the public cloud is standardisation of service, the evidence from the results here support this idea, where there is a lack of trust in a flexible service level agreement that would support governance. The public cloud service is provided by the CSP; however, the cloud and associated infrastructure is provided by a cloud provider (CP) as a third party. It is clear from these results that the government do not have confidence because they do not trust that they will be given sufficient knowledge and control over these third parties.

Sub cloud factors of governance where there was a level of trust included *clarity of roles and responsibilities*. This means that the government trust the CSP in terms of clarity of roles and responsibilities for governance which means that they feel that they can trust that the CSP

will be clear about who is responsible for what aspects of governance. The same was found to be true for *auditing and measuring the CSP* for governance and *governance during migration*. However, the latter two are expected from a CSP by all types of orgasnisation and are not a particular concern to government (see Figure 5-3). Overall, there is a high level of mistrust that the CSP will offer provision for governance that are a particular interest for government. Moreover, the results have shown that this level of mistrust is not reflected in trust of the CSP generally.

Because the results clearly show levels of trust and levels of mistrust, this study has shown that it is necessary to address trust not just generally, but in relation to cloud factors and sub cloud factors in order to fully understand which aspects of the cloud are a concern in relation to trust. This has been evidenced by the fact that there are certain areas of governance where there is trust, and certain where there is mistrust, reflecting certainty in the opinions of government.

Figure 5-3: Trust and Sub Cloud Factors of Governance



5.3.1.2 Trust with other relationship factors (governance) (Spearman correlation)

Table 5-2: Trust with other relationship factors (governance) (Spearman correlation)

Relationship factors	Risk	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Trust	weak	weak	weak	moderate	moderate	weak	NC	weak

There were positive moderate correlations between the government trusting the CSP about governance and having the perception that they can negotiate and collaborate for governance, evidenced by Spearman correlations of 0.508** and 0.595. Overall, there was a statistically significant positive correlation shown between trust and collaboration for most sub cloud factors of governance. These included *Your need to have knowledge and control over data and processes*, *Assurance about other cloud tenants* and *Knowledge and control over third party issues*, this means that trust and the ability to effectively collaborate are essential for these sub cloud factors.

There was found to be a positive correlation between trust of the CSP and perception of a positive reputation for the cloud factor of governance generally, although this was weak at 0.277* (Spearman). Moreover, the correlation between trust and reputation was non – existent for all sub cloud factors of governance except *governance during migration*. Overall these results show that where the government mistrust or trust the CSP it does not mean that they perceive a negative or positive reputation respectively for governance.

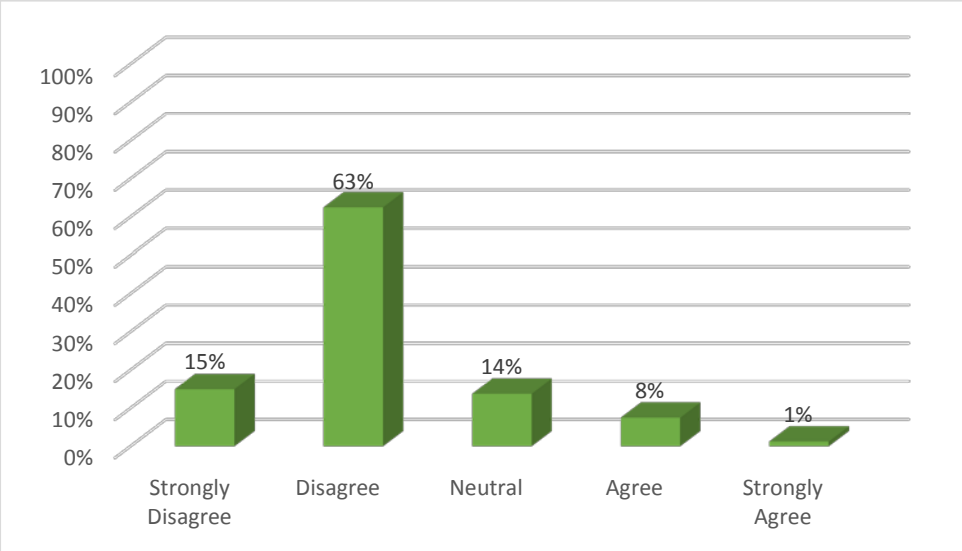
5.3.1.3 Trust and Compliance

There was a high level of disagreement with the idea that the government trust the CSP in relation to compliance. This enforces the idea that although the respondents felt confident that they trust their CSP generally, there was a high level of mistrust for compliance as a cloud factor. This was evidenced by 63 percent disagreeing that they trust their CSP in relation to compliance. Although it should be noted that 14 percent were neutral, but only 9 percent in total were in agreement that they could trust in relation to compliance.

It is important to note at this point that governance and compliance cloud factors would be of particular concern to government as the literature suggests, governance because government need a certain level of knowledge and control over data and systems, and compliance because governments have to be compliant with their own and international requirements (see Figure 5-4).

There was a much higher level of mistrust in the compliance that is offered by the CSP than there was for governance. Compliance requirements for government are unique and specific to government, and if a government cannot achieve compliance it would go against their own regulation and laws. Therefore, this mistrust in compliance is a contributing factor to government reluctance in the public cloud.

Figure 5-4: Trust in Relation to Compliance (Q2B)



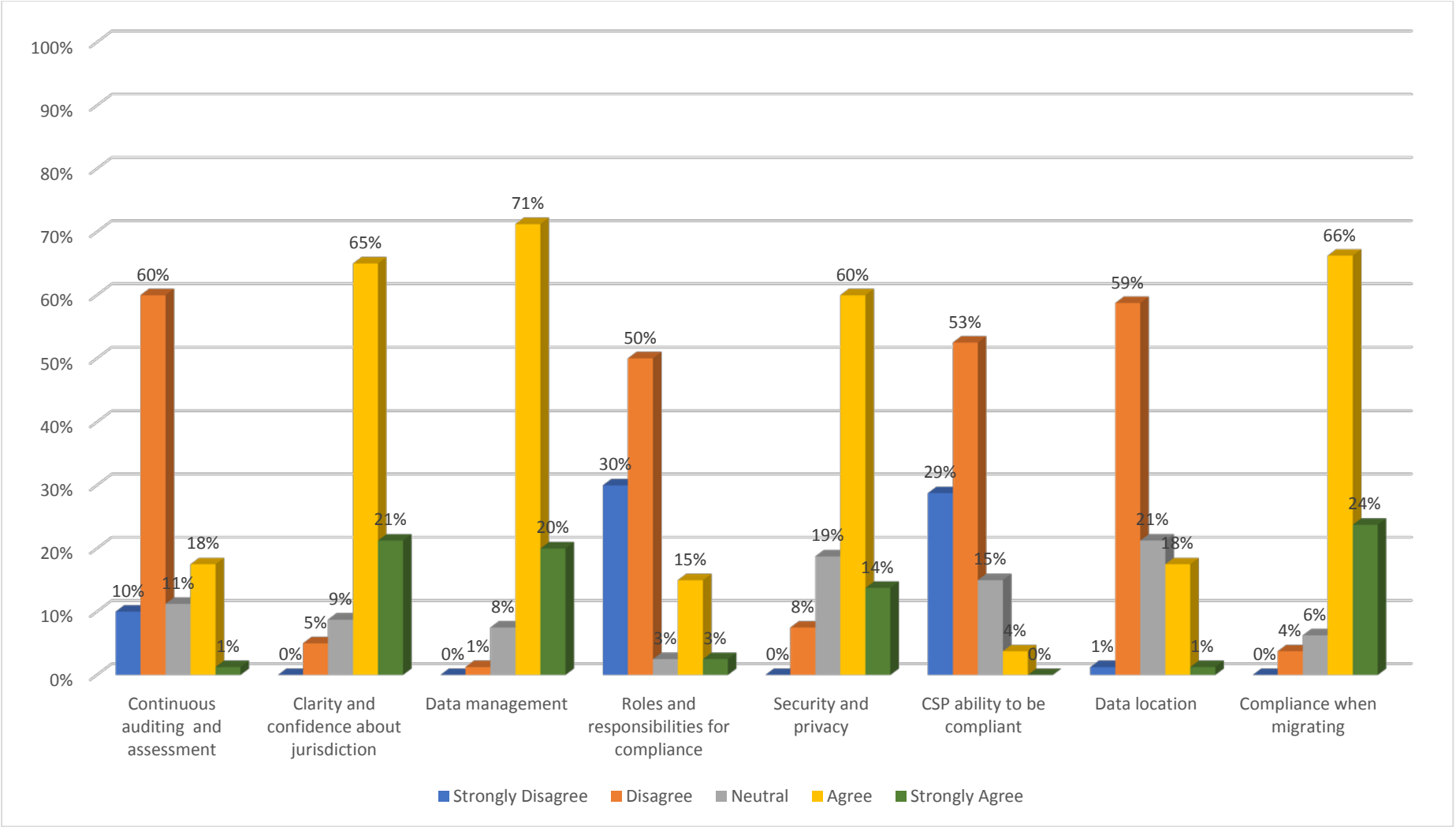
5.3.1.4 Trust and Sub Cloud Factors of Compliance

Compliance is an important issue for government because they have to be compliant with local and international laws and regulations. The results show that the government do not trust their CSP in relation to the CSP's ability to be compliant. There was also a lack of trust in the area of *data location*, this is also important as part of achieving compliance. There was further concern in the area of compliance which was evidenced by the fact that the government did not trust the CSP in the area of roles and responsibilities for ensuring compliance. Another area that is an important part of ensuring compliance is continuous

auditing and assessment were there was also a low level of trust (see Figure 5-5). However, there was a high level of trust in compliance during migration to the cloud.

Despite the general mistrust in the area of compliance, the government respondents did feel that they could trust their CSP in relation to clarity and confidence about jurisdiction, jurisdiction is a specific concern for compliance because compliance requires that data should be located in particular locations and that there is knowledge about where data is located. Moreover, there was a high level of trust in data management and security and privacy as a part of compliance.

Figure 5-5: Trust and Sub Cloud Factors of Compliance



5.3.1.5 Trust with other relationship factors (Compliance) (Spearman correlation)

Table 5-3: Trust with other relationship factors (compliance) (Spearman correlation)

Relationship factors	Risk	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Trust	Moderate 0.533**	NC	NC	moderate 0.516**	Strong 0.662**	Weak 0.334**	NC	Strong 0.637**

A lack of trust in certain areas of compliance may affect other relationship factors, for example a lack of trust may affect the perceived ability to negotiate or collaborate with the CSP in these same sub cloud areas. In reference to negotiation, a positive and moderate correlation of 0.516** between trusting the CSP in relation to compliance and being able to negotiate compliance was found. Both the frequencies for trust with compliance and negotiation with compliance showed a high level of disagreement. Therefore, in relation to compliance where the government mistrust the CSP they also feel that they cannot negotiate with the CSP.

As for the sub cloud factors of compliance, statistically significant correlations were found between trusting the CSP and being able to negotiate (understand requirements) with the CSP in relation to *Continuous auditing and assessment*, and given there was a high level of mistrust for this sub cloud factor it means that where the government mistrust the CSP about *continuous auditing and assessment*, they also feel that they cannot negotiate (understand requirements) in the same area, the same was found to be true for *roles and responsibilities for compliance*. The remaining sub cloud factors of *Data management*, *Data location* and *Compliance when migrating* were shown to have no or weak correlations with no statistical significance in these correlations between trust and negotiation. Therefore, for areas that are a particular concern for government, trust has less of an effect on negotiation.

The strong link between trust and collaboration is evidenced by the fact there were strong correlations between trusting the CSP in relation to compliance and the government having the perception that they have the ability to collaborate with the CSP about compliance as well as having a perception of a positive reputation. This was evidenced with a positive strong correlation of 0.662** and 0.637** respectively (see Table 5.3). Positive correlations

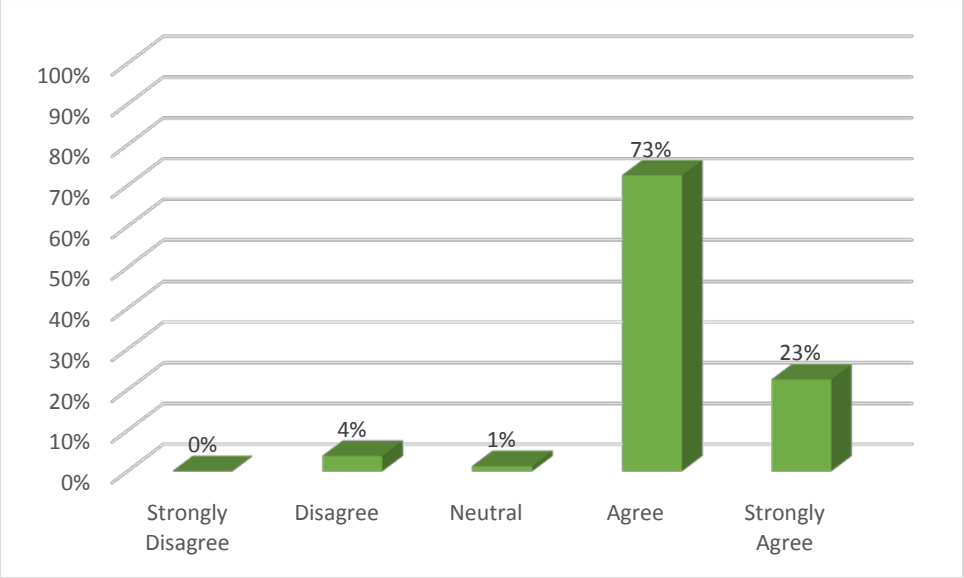
between trust and collaboration were found for 5 out of the 8 sub cloud factors for compliance which included *Continuous auditing and assessment, Clarity and confidence about jurisdiction, Data management, Roles and responsibilities for compliance* and *Security and privacy*. Overall, this means that for these areas of the cloud where there was trust there was an associated ability to collaborate and a positive perception of reputation, or where there was mistrust there was the idea that they could not collaborate or perceived a negative reputation. Therefore, because collaboration is required to achieve compliance it is important that the government trust the CSP.

The above correlation between trust and reputation for compliance could not have been related to having sufficient information about the CSP because there was no statistically significant correlation between trust and sufficient information about CSP in relation to compliance.

5.3.1.6 Trust and Security and Privacy

In response to whether or not the respondents trust the CSP in relation to security and privacy it was found that the majority, 96 percent, agreed that they trust their provider, with more than 23 percent strongly agreeing, this was a very strong result in comparison to only 4 percent who disagreed. These results were in stark contrast for the results for governance and compliance. This indicates that security and privacy is something that is not an issue generally for the respondents, that they generally trust their CSP (see Figure 5-6). These results are apparently in contrast to much literature which suggests that customers have trust issues with security and privacy.

Figure 5-6: Trust in Relation to Security and Privacy (Q2C)



5.3.1.7 Trust and Sub Cloud Factors of Security and Privacy

Continuing with the theme that has emerged from the other cloud and sub cloud factors, where there is a low level of trust it is related to areas of the cloud that are particularly important to government, these particular concerns have been identified in the literature about government concerns about the cloud. An example of this was a high level of mistrust, at 63 percent disagreement and 20 percent strong disagreement, in relation to security of third parties. The issue of mistrusting the CSP in relation to third parties was also a trust issue for governance. Therefore, here there is evidence to suggest that third parties is a concern generally for government.

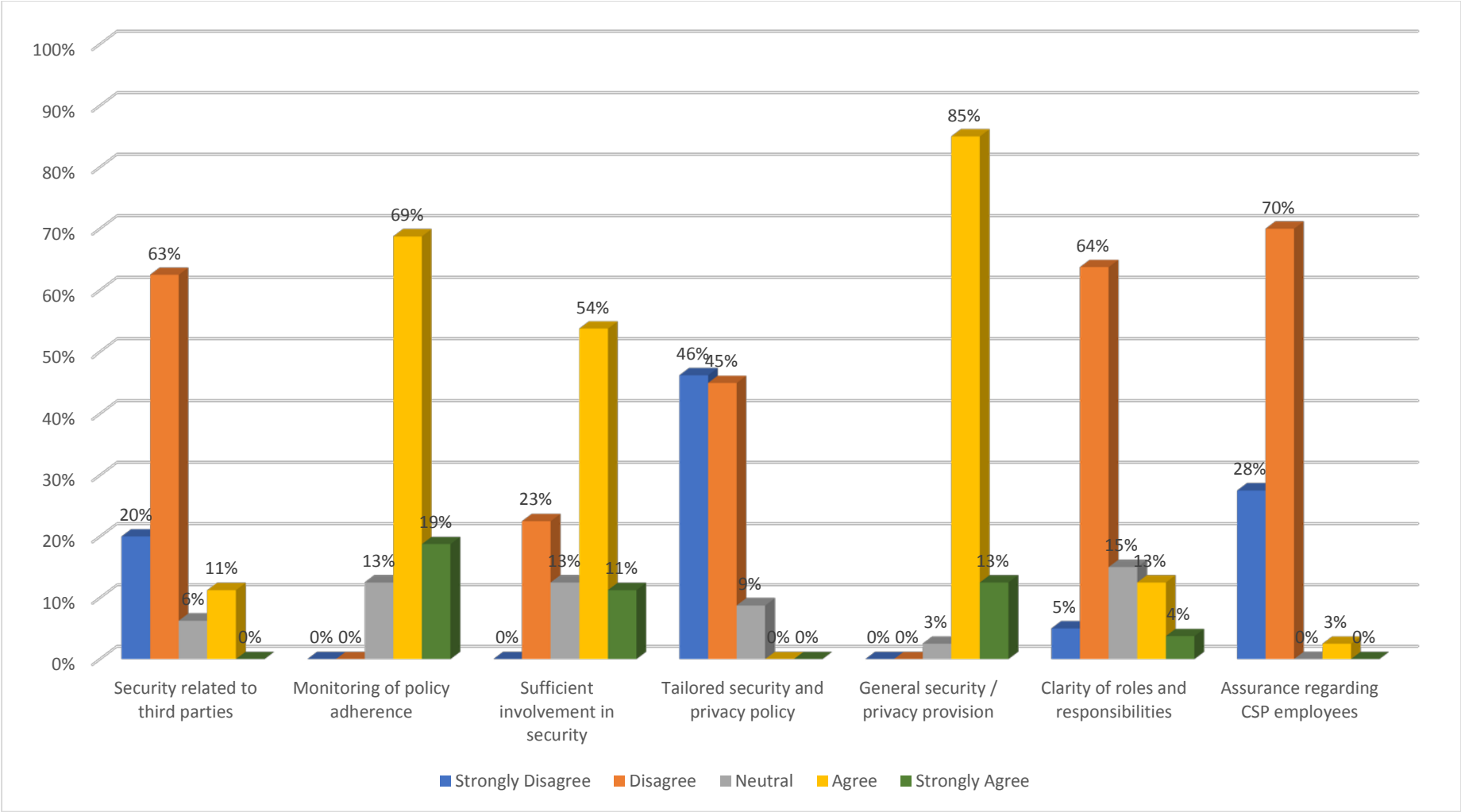
In reference to a *tailored security and privacy and policy* there was a very high level of mistrust with 46 percent disagreeing and 45 percent strongly disagreeing with this idea. This closely relates to the idea found in the results cited in the above that there is a level of mistrust regarding a flexible agreement. Overall, therefore, there is a mistrust in the idea of flexibility on the part of the CSP in regard to agreements and policies.

Security is an area that is the responsibility of all parties. Governments would be expected to have their own security and privacy protocols that they would have to follow, however, they do not trust the CSP in terms of establishing *clarity about the roles and responsibilities* for

security and privacy. A significant 64 percent felt they could not trust the CSP in this regard. Again, this is something that is beyond the government's control.

In addition to not having confidence that responsibilities for security are not clearly established, the government also mistrusted the CSP in reference to *assurance regarding CSP employees*, where 70 percent disagreed and 28 percent strongly disagreed with this idea. Therefore, almost all respondents were concerned about the employees of the CSP in relation to security. Together with the high level of mistrust about third parties, it is clear that the government have a high level of concern about parties or individuals that they are not aware of, this have been evidenced for governance and security and privacy.

Figure 5-7: Trust and Sub Cloud Factors of Security and Privacy



5.3.1.8 Trust with other relationship factors (Security and Privacy) (Spearman correlation)

Table 5-4: Trust with other relationship factors (security and privacy) (Spearman correlation)

Relationship factors	Risk	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Trust	NC	NC	NC	weak 0.310**	weak 0.284*	NC	Weak 0.283*	NC

5.3.1.9 Trust with Security and Privacy

There was a positive weak correlation between trust in security and privacy and the ability to negotiate and collaborate for security and privacy. This was also found to be the case for having sufficient information about the CSP. Therefore, trust has the same effect on the ability to collaborate for security and privacy than it does on the ability to negotiate for security and privacy. So it can be said that trust is a determining factor in decisions to be made about the public cloud so far as it affects negotiation and collaboration.

No statistically significant correlation was found between trust and the perception of a positive reputation for security and privacy. This is an important finding because the literature suggests that perception of a positive reputation is one of the key factors for the willingness to adopt the cloud and it would be expected that if a CSP had a positive reputation for security and privacy they would trust the CSP. Therefore, trust is not a determining factor on adoption as a result of its affect on reputation.

For the relationship between trust and negotiation, the sub cloud factors that received positive correlations were *Tailored security and privacy policy* (0.453**) and *Clarity of roles and responsibilities* (0.415**). For collaboration, only 2 out of the 7 were found to have a positive correlation, however, even these were moderate, they also included *Tailored security and privacy policy* (0.468**) and *Clarity of roles and responsibilities* (0.549**). Therefore, trust has an effect on the ability to negotiate and collaborate only for these two sub cloud factors. For sufficient information (reputation domain) the sub cloud factors of security and privacy only *Clarity of roles and responsibilities* was found to have a significant moderate correlation (0.400** Spearman) and for reputation the only correlation was for *Clarity of roles and*

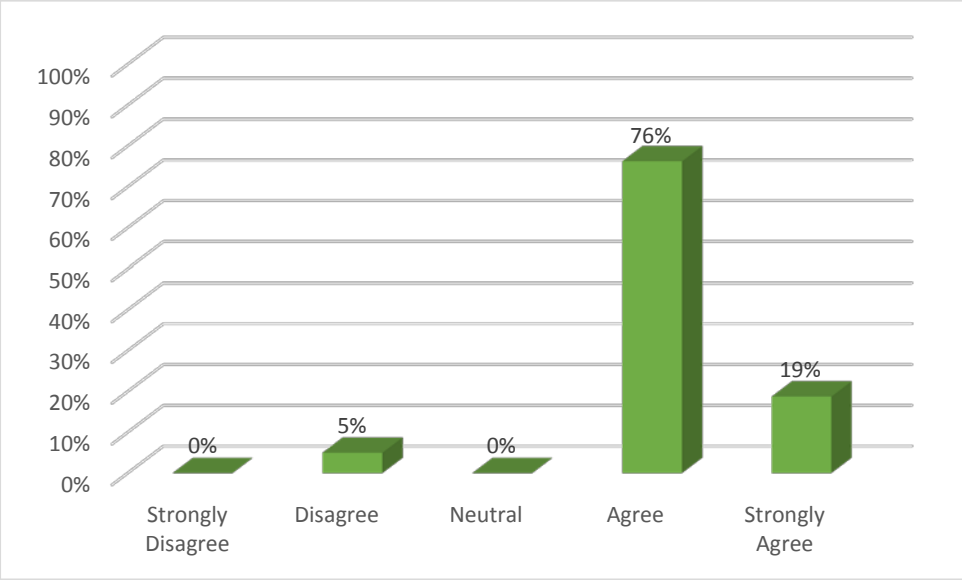
responsibilities where a positive strong correlation was found (0.695 ** Spearman correlation).

Overall, therefore, where trust is analysed against the other relationship factors of negotiation, collaboration and reputation although there was little correlation found in relation to security and privacy, for the sub cloud factor *Clarity of roles and responsibilities* there was consistently a correlation. This means that trust in this sub cloud factor results in a perceived ability to negotiate and collaborate and the perception of a positive reputation.

5.3.1.10 Trust and Performance and Offering

In consideration of the government trusting the CSP in relation to performance and offering generally, there was a high level of trust with 76 percent agreeing and 19 percent strongly agreeing and only 5 percent disagreed (see Figure 5-8).

Figure 5-8: Trust in Relation to Performance and Offering (Q2D)



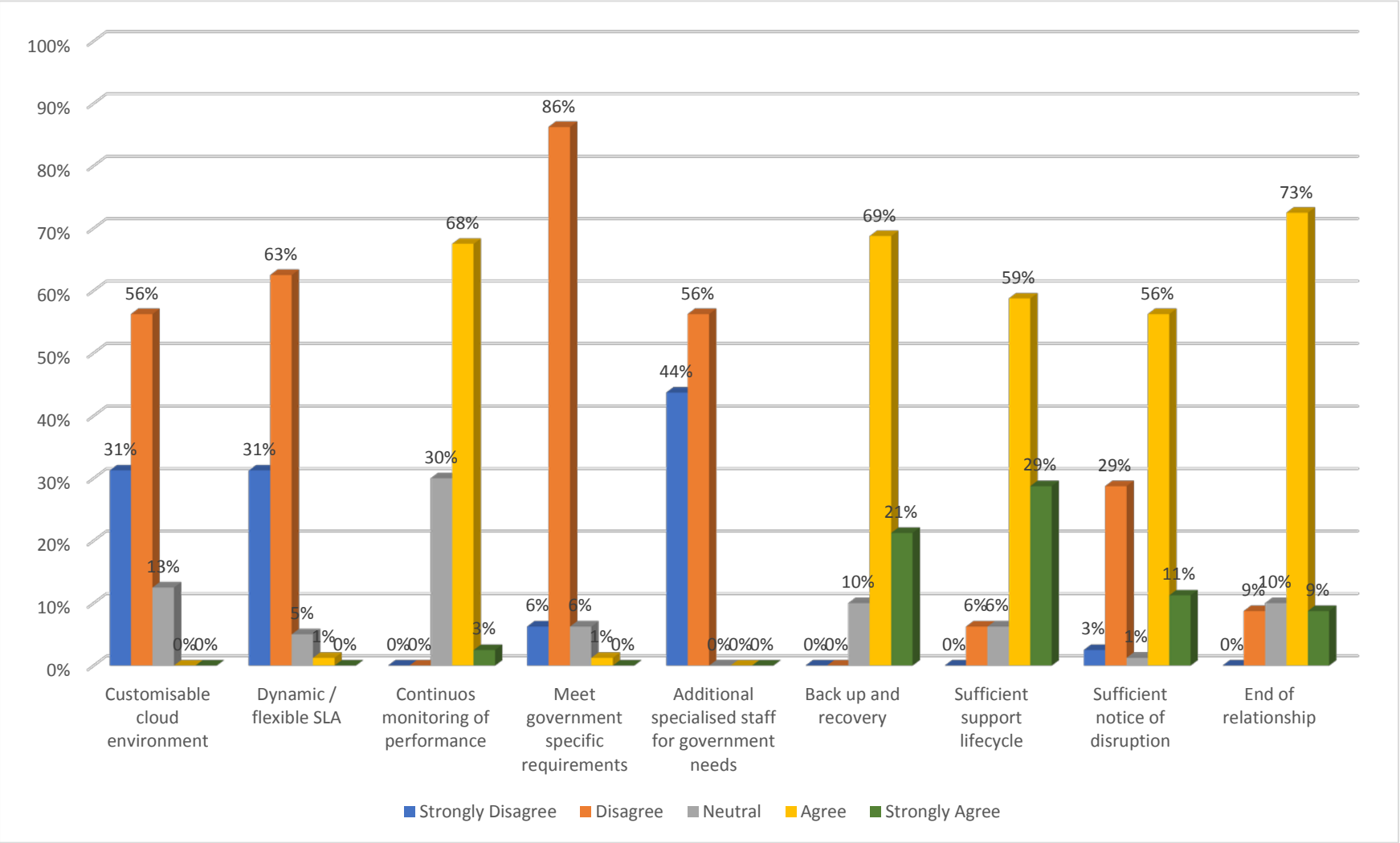
5.3.1.11 Trust and Sub Cloud Factors of Performance and Offering

There was a high level of trust for those areas that are related to performance specifically. This included trust where the relationship ended and sufficient notice of any disruption, moreover, the majority of the government respondents trust that they will receive sufficient support from their CSP (see Figure 5-9).

Again, as with other cloud factors, a level of mistrust was found for the associated sub cloud factors that were particularly relevant to government. For *meet government's specific governance requirements* where 86 percent disagreed (see Figure 5-9). The other areas where

there was a high level of mistrust included *specialised staff for government needs* with all of the government respondents disagreeing with the idea that they trust the CSP in this area. Moreover, towards achieving governance, government need to have specialised staff inside the CSP organisation as well as a dynamic / flexible SLA, however, a high level of mistrust was expressed for these sub cloud factors, with 56 percent disagreement and 44 percent strong disagreement, and 63 percent disagreement and 31 percent strong disagreement respectively (see figure 5.9). Again, where requirements are considered that are of particular relevance to government, a level of mistrust is perceived.

Figure 5-9: Trust and Sub Cloud Factors of Performance and Offering



5.3.1.12 Trust with other relationship factors (Performance and Offering) (Spearman correlation)

Table 5-5: Trust with other relationship factors (performance and offering) (Spearman correlation)

Relationship factors	Risk	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Trust	weak 0.380**	NC	weak 0.231*	weak 0.238*	weak 0.271*	weak 0.239*	NC	NC

There was a positive, however, weak correlation between trust in the CSP's performance and offering and ability to negotiate and collaborate for performance and offering. Because most of the respondents agreed that they trusted the CSP in relation to performance and offering, this means that where they trust their CSP in relation to performance and offering, to a certain extent, they feel that they can negotiate and collaborate for the same cloud factor. Again, trust is therefore, a factor that has a bearing on the ability to negotiate and collaborate to a specific cloud factor, in this case Performance and Offering, as was also the case for Security and Privacy.

The following sub cloud factors of performance and offering were found to have a correlation between trust and collaboration: *Dynamic / flexible SLA* (0.455**) and *Additional specialised staff for government needs* (0.438**), both of which there was a strong level of disagreement for trust. Therefore, for these sub cloud factors, which are a particular concern or relevance for government, a lack of trust is associated, to a certain extent, with a perceived lack of ability to collaborate. Here, therefore, there are two issues about adoption of the cloud that are related to sub cloud factors that government need to be concerned about, firstly they cannot trust the CSP and secondly, they cannot collaborate with the CSP. The opposite is found to be true for the sub cloud factors *Sufficient notice of disruption* and *End of relationship*, where a positive perception of trust is associated with a perceived ability to collaborate. From other results for these sub cloud factors there is always a positive perception. These are seen as standard conditions of a contract and it is expected that a CSP offers assurances about them as standard which has been reflected in the positive results.

There was no statistically significant correlation between trust and perception of positive reputation and having sufficient information about the CSP in relation to the cloud factor of

performance and offering. Therefore, trust was not related to reputation, which is different to what is expected because there should be a correlation between trust and reputation, however, this was not the case where performance and offering were concerned. A correlation that was found in the sub cloud factors of performance and offering was *Customisable cloud environment,* which had a moderate correlation (0.462**) Spearman. For this particular sub cloud factor there was a low perception of trust which is therefore, associated with a negative perception of ability to negotiate, the was also the case for *Dynamic / flexible SLA.*

Overall, therefore, trust has a determining effect, or is determined by other relationship factors, especially negotiation and collaboration, for sub cloud factors that are a particularly relevant to government. From this idea, which has already been determined from previous results, levels of concern or confidence are affect by these government-specific concerns.

Table 5-6: Trust and Sufficient Information with Performance and Offering 2D 16D

Sub cloud Factors of Performance and Offering	**Correlation (Spearman)**
Customisable cloud environment	0.538 (**) moderate correlation
Dynamic / flexible SLA	0.345 (**) weak correlation
Continuous monitoring of performance	0.333 (**) weak correlation
Back up and recovery	0.261 (*) weak correlation
Sufficient support lifecycle	0.463 (**) moderate correlation
Sufficient notice of disruption	0.490 (**) moderate correlation
End of relationship	0.358 (**) weak correlation
	No correlation / No statistically significant correlation
Meet government specific requirements	0.004
Additional specialised staff for government needs	0.212

In the case of performance and offering where the respondents are asked about trust in this area generally, there was a very high level of trust, however, where respondents are asked about trust in relation to the specific sub cloud factors of performance and offering there was

a variation in levels of trust, in relation to some areas there was a high level of mistrust. This reveals that the respondents demonstrate a high level of certainty about certain ideas within the cloud factors. This has been shown to be the case for all of the cloud factors for each of the relationship factors. Where respondents demonstrate clear distinctions between trusting and not trusting CSPs in relation to certain sub cloud factors, it reveals a high level of confidence in their opinion. Moreover, in reference, for example, to trusting the CSP in relation to performance and offering there was a very high level of trust in relation to this generally, however, for some of the sub cloud factors there was a high level of mistrust. Not only does this demonstrate that respondents show a level of certainty in relation to certain issues it also shows that there is a clear need to not only ask about cloud factors generally but to look at the individual aspects of cloud factors, namely the sub cloud factors.

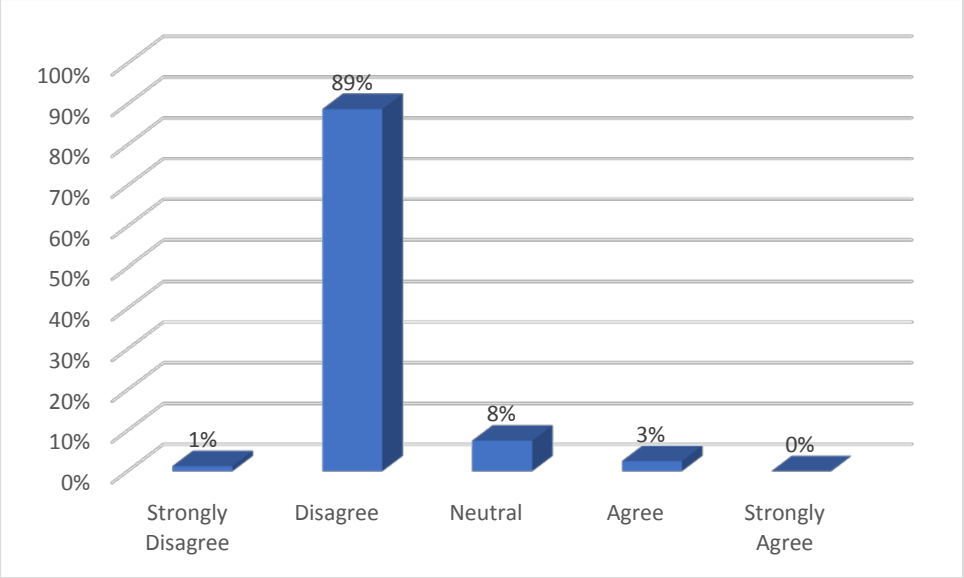
5.4 Risk Domain – Relationship Factor

In this section, the results for risk are addressed whereby it is analysed against cloud and sub cloud factors.

5.4.1 Risk

Respondents were asked if they do not perceive a risk with their cloud service provider. The vast majority of the respondents (89 percent) disagreed with the idea that they did not perceive a risk and only 3 percent agreed, less than the 8 percent that responded neutral, this means that they perceived a risk (see Figure 5-10). This result is in stark contrast to trust where there was an overall positive perception. This means that although the government perceive a risk, they do trust the CSP.

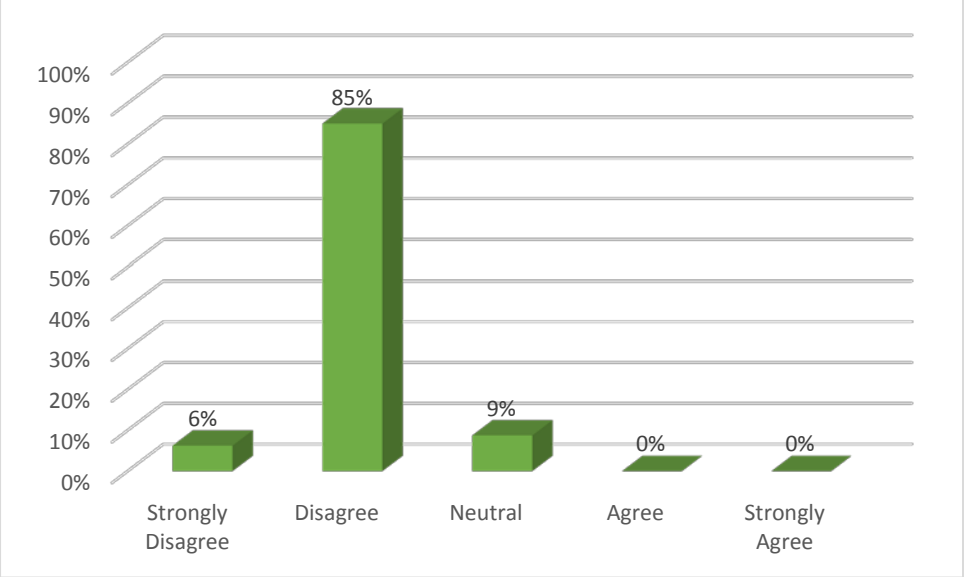
Figure 5-10: Risk Perception



5.4.1.1 Risk and Governance

The results in the above show that there is a high level of perception of risk generally, this idea was also found where the respondents were asked about risk in relation to governance. The vast majority of respondents, 85 percent, perceived a risk in relation to governance and none of the respondents did not perceive a risk (see Figure 5-11).

Figure 5-11: Risk in Relation to Governance (Q4A)

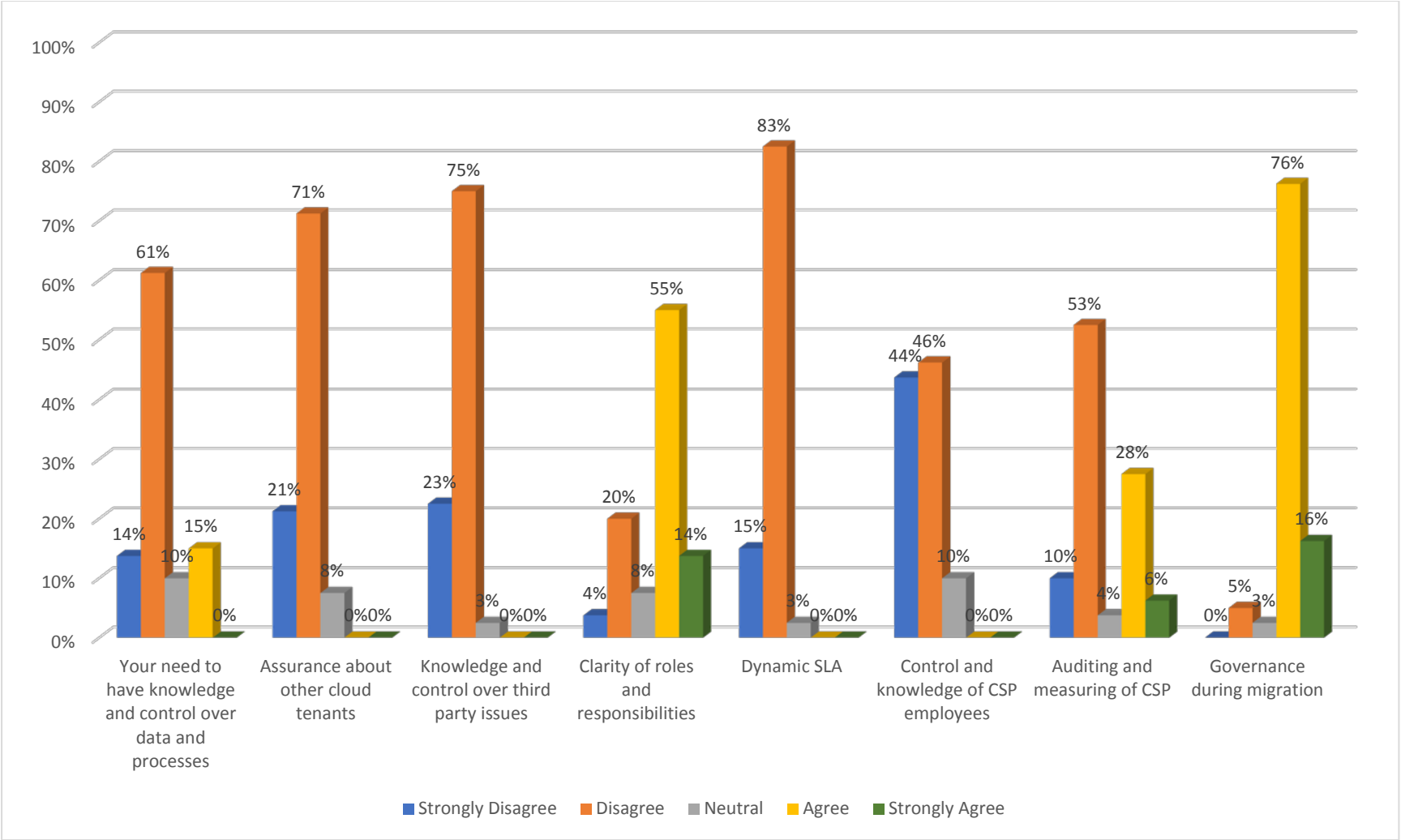


5.4.1.2 Risk and sub Cloud Factors of Governance

For most of the sub cloud factors of governance there was a high level of disagreement. This high level of disagreement was especially high for a *Dynamic SLA* with 83 percent of respondents disagreeing and 15 percent strongly disagreeing, *knowledge and control over third parties* 75 percent and 23 percent and *assurance about other cloud tenants* at 71 percent and 21 percent respectively (see Figure 5-12). Again, as a recurring finding of this study, where there seems to be an issue is with the sub cloud factors of governance that are especially a concern or relevance to government.

There were only two sub cloud factors where there was a higher level of agreement that the respondents did not perceive a risk which were *governance during migration* at 76 percent agreeing and 16 percent strongly disagreeing, and *clarity of roles and responsibilities* with 55 percent and 14 percent respectively.

Figure 5-12: Risk and Sub Cloud Factors of Governance



5.4.1.3 Risk with other relationship factors (Governance) (Spearman correlation)

Table 5-7: Risk with other relationship factors (governance) (Spearman correlation)

Relationship factors	Trust	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Risk	weak 0.297**	NC	weak 0.227*	moderate 0.423**	weak 0.300*	NC	moderate 0.416**	Weak 0.360**

There was a positive moderate correlation between risk and negation in relation to governance, this was evidence by a 0.423 (**) Spearman correlation, the same was found to be true for sufficient information with a moderate correlation of 0.416** (see Table 5.7).

Because there were positive correlations for sub cloud factors that were standard and sub cloud factors that are considered to be of particular concern to government, where both positive and negative perceptions of risk were found, this means that there is a correlation between a negative perception of risk and a perceived inability to negotiate and a correlation between positive perception of risk and ability to negotiate, both for governance.

Although there was a correlation between risk and reputation, it was weak and there were no significant correlations for the associated sub cloud factors of reputation.

There was no statistically significant correlation between risk and specifying requirements in relation to the cloud factor of governance. Moreover, out of the 8 sub cloud factors only 2 showed a correlation, however, they were weak. Therefore, the perception of a risk for governance is not associated with the government's ability to specify governance requirements.

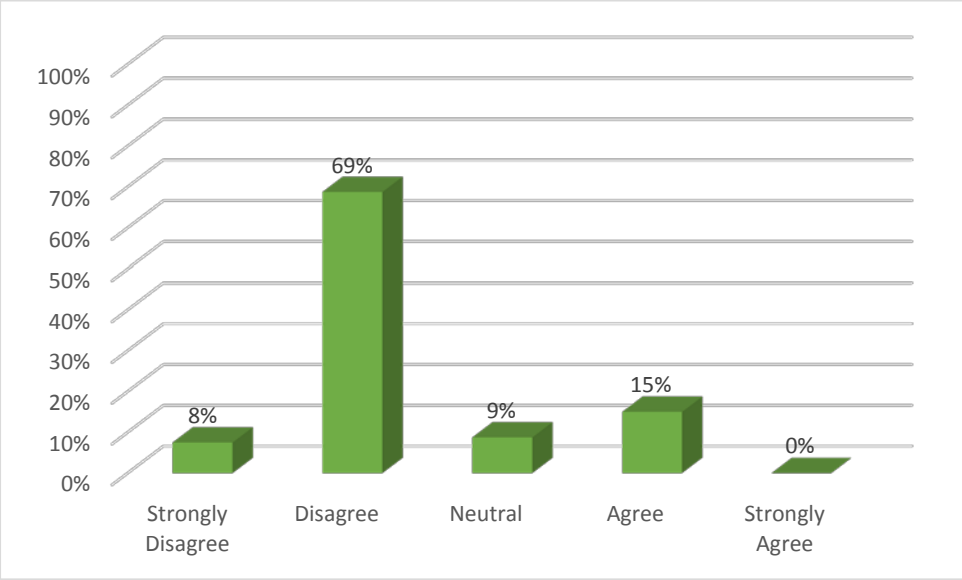
Although no correlation was found between risk and effectively communicate there were positive correlations for five of the eight sub cloud factors of governance between risk and effective communication. However, there was no pattern in terms of the sub cloud factors that would be of particular concern to government, some of these sub cloud factors that showed a correlation were those that are of a particular concern to government and some were not. This means that for sub cloud factors that show a low perception of risk there is an associated perceived ability to be able to communicate during collaboration, and the opposite was found

to be true for those sub cloud factors where a risk was perceived. These findings further enforce the idea that risk is linked to the governments perceived ability to effectively communicate.

5.4.1.4 Risk and Compliance

The idea of perceiving a risk in relation to a specific cloud factor was also found to be true in relation to compliance where most of the respondents, 69 percent, disagreed and 8 percent strongly disagreeing, with idea that they did not perceive a risk in relation to compliance. Only 15 percent of the respondents agreed that they did not perceive a risk, and 9 percent responded neutral (see Figure 5-13).

Figure 5-13: Risk in Relation to Compliance (Q4B)

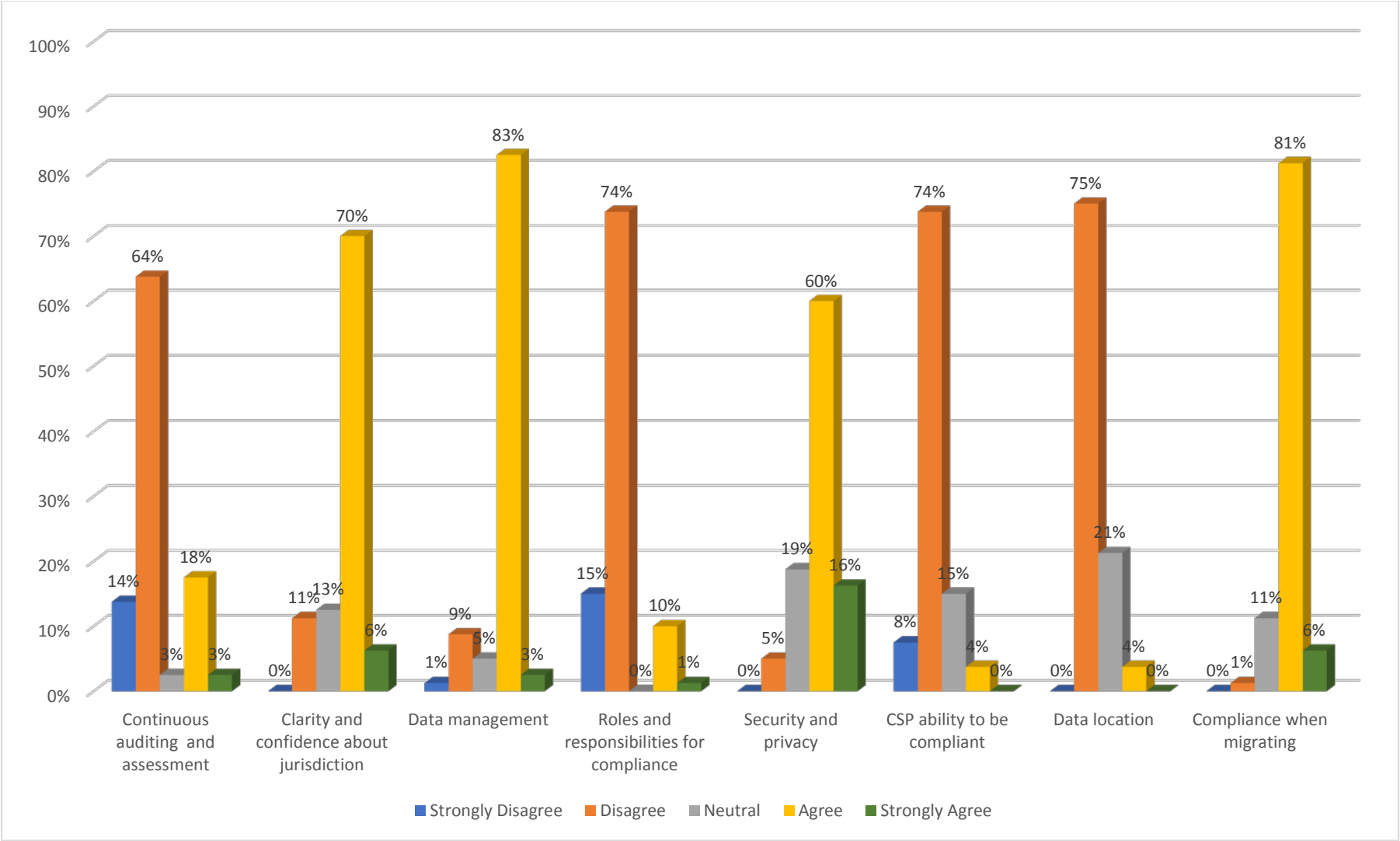


5.4.1.5 Risk and Sub Cloud Factors of Compliance

Despite the fact that there was shown to be a high perception of risk in relation to compliance generally as a cloud factor, where there is an examination of the results for the sub cloud factors of compliance there is a significant amount these factors where a risk is not perceived. Specifically, for *Clarity and confidence about migration, Data management, Security and privacy* and *Compliance when migrating* there was a low perception of risk. However, there were sub cloud factors of compliance where a risk was perceived which included *Data location, CSP ability to be compliant, Roles and responsibilities for compliance* and *Continuous auditing and assessment.*

Therefore, the concern about sub cloud factors that are of particular relevance to government is also found here. Data location is especially a concern for government when it comes to achieving compliance, moreover, the government should have confidence in the CSP that they will be able to be compliant. Because there was a perception of risk in relation to the roles and responsibilities for compliance this means that there could be a lack of clarity about who is responsible for compliance. Finally, there is a perception of risk in relation to continuous auditing and assessment, this means that the government respondents feel that there is a risk that a continuous auditing and assessment for compliance is not carried out (see Figure 5-14).

Figure 5-14: Risk and Sub Cloud Factors of Compliance



5.4.1.6 Risk with other relationship factors (Compliance) (Spearman correlation)

Table 5-8: Risk with other relationship factors (compliance) (Spearman correlation)

Relationship factors	Trust	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Risk	moderate 0.533**	NC	weak 0.249*	moderate 0.447**	moderate 0.426**	NC	NC	moderate 0.430**

For compliance, there were positive and moderate correlations between risk and trust, ability to negotiate, effectively collaborate and positive reputation. This means that risk is linked to these relationship factors where compliance is concerned.

In reference to the link between risk and reputation, for five out of the eight sub cloud factors of compliance there were positive correlations. Four of these correlations were for sub cloud factors that are considered to be of a particular concern for government as evidenced by the literature and results in this study. The result show that the perception of risk for compliance, whether high or low, is correspondingly associated with a perception of reputation of the CSP in relation to compliance, whether negative or positive. Therefore, reputation could have a bearing on the decision to adopt the public cloud.

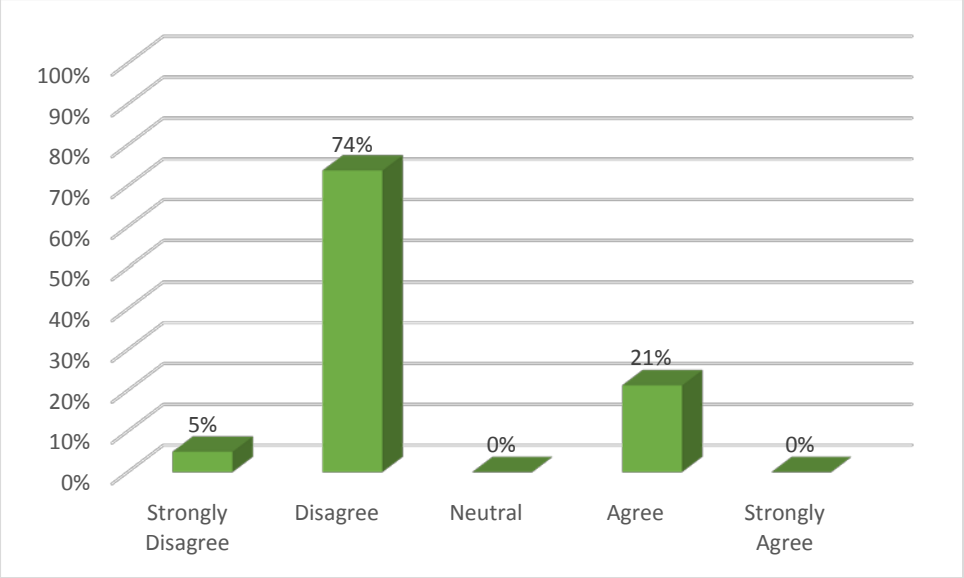
A weak correlation was found between risk and understand requirements, and the associated sub cloud factors had either weak or no correlations. Moreover, no correlation was found for compliance between risk and specify requirements and no noteworthy correlation for the associated sub cloud factors. Therefore, risk is not related to the perception that requirements are being understood. As for risk and effective communication there was also no correlation, therefore, any risk that the government may perceive about compliance cannot be attributed to the ability of the government to effectively communicate for compliance.

For the relationship between risk and negotiation for all of the sub cloud factors of compliance, except one, there were positive correlations, most of them moderate or strong, in particular *Data location* had the highest correlation at 0.6647* Spearman. The results indicate that where there is either a high or low perception of risk, it is correspondingly associated with a high or low perception of the ability to negotiate for compliance.

5.4.1.7 Risk and Security and Privacy

The perception of risk was asked in relation to all four of the main cloud factors. Where the respondents were asked about the perception of risk in relation to security and privacy the results showed similar results to governance and compliance where 74 percent disagreed that they did not perceive a risk. However, it is important to note that 21 percent of the respondents agreed that they did not perceive a risk (see Figure 5 15).

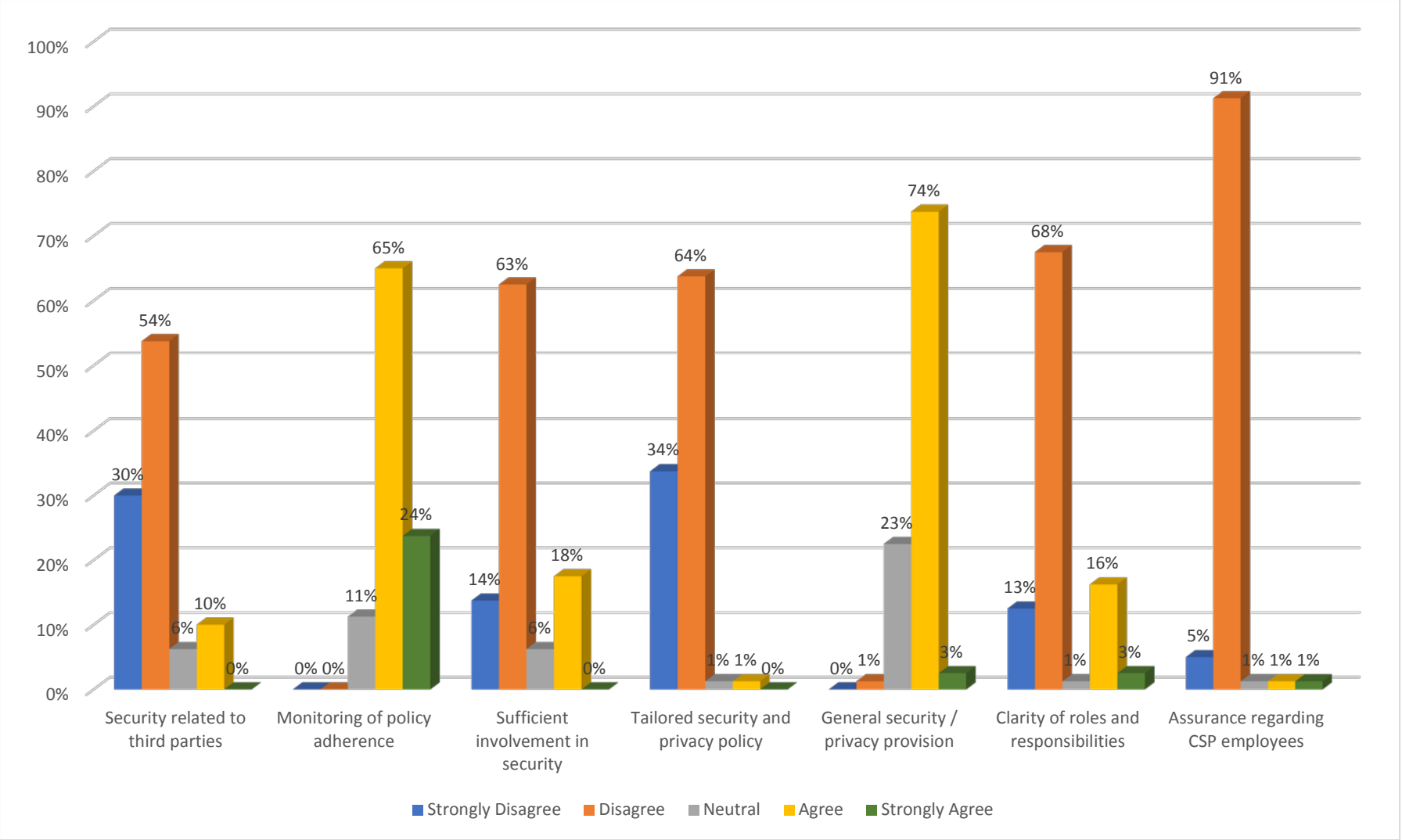
Figure 5-15: Risk in Relation to Security and Privacy (Q4C)



5.4.1.8 Risk and Sub Cloud Factors of Security and Privacy

In reference to the sub cloud factors for security and privacy there was evidence of a perception of risk in relation to *Assurance regarding CSP employees* where 91 percent disagreed that they did not perceive a risk and 5 percent strongly disagreed, *Clarity of roles and responsibilities* whereby 68 percent disagreed, *Security related to third parties* where 54 percent disagreed and 30 percent strongly disagreed, and finally *Tailored security and privacy policy* where 64 percent disagreed with 34 percent strongly disagreeing (see Figure 5-16).

Figure 5-16: Risk and Sub Cloud Factors of Security and Privacy



Where there was a high level of agreement, which means that the respondents did not perceive a risk was the highest for *General security / privacy provision* with 74 percent agreeing and 3 percent strongly agreeing, followed by *Monitoring of policy adherence* with 65 percent and 24 percent agreeing and strongly agreeing respectively, and finally, *Sufficient involvement in security* at 18 percent 0 percent respectively.

Again, this is a recurring idea there is a high perception of risk in areas that would be of particular concern or relevance to government, although it is important to note that all of these sub cloud factors are important to government, the additional requirement to know about third parties is something that governments would be obligated to know about according to law and also for security purposes, as they are obligated to do everything possible to protect citizen data. Tailored security and privacy policy is also something that is required by government.

5.4.1.9 Risk with other relationship factors (Security and Privacy) (Spearman correlation)

Table 5-9: Risk with other relationship factors (security and privacy) (Spearman correlation)

Relationship factors	Trust	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Risk	NC	Moderate 0.468**	weak 0.309**	NC	NC	NC	NC	NC

In consideration of the relationship between risk and other relationship factors only risk and specify requirements showed a moderate positive correlation, this was followed by risk and CSP understand requirements which showed a weak correlation (see Table 5.9). No correlations were find between risk and other relationships for security and privacy.

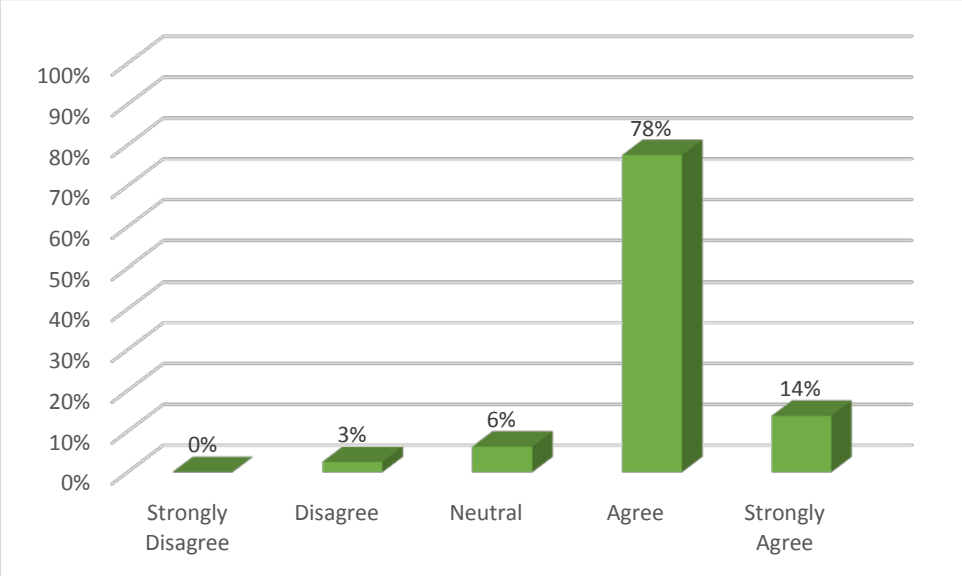
There was no statistically significant correlation between risk and collaboration in relation to security and privacy. For the sub cloud factors, there were either weak or no correlations. The only sub cloud factor worth a mention is *Clarity of roles and responsibilities* with a Spearman correlation of 0.685**. There was also no correlation in the relationship between risk and reputation, but as with risk and collaboration, the only sub cloud factor where there was a correlation between risk and reputation was *Clarity of roles and responsibilities* with a correlation of 0.654**.

Where the study determined if there was a relationship between a perception of risk for security and privacy and the perceived ability to effectively communicate for security and privacy, very little correlation was found. Therefore, a perception of risk for security and privacy, negative or positive, is not linked to the perceived ability to effectively communicate for security and privacy.

5.4.1.10 Risk and Performance and Offering

Where respondents were asked about the perception of risk in relation to performance and offering the results were the opposite to the aforementioned cloud factors of governance, compliance and security and privacy. There were 78 percent of respondents who agreed with the idea that they do not perceive a risk in relation to performance and offering, in addition to this there were 14 percent who strongly agreed with this idea, only 3 percent disagreed. This was in stark contrast to the other three cloud factors where a majority perceived a risk (see Figure 5-17).

Figure 5-17: Risk in Relation to Performance and Offering (Q4D)



5.4.1.11 Risk and Sub Cloud factors of Performance and Offering

For the sub cloud factors of performance and offering there was a perception of risk for a *Customisable cloud environment* with 78 percent disagreeing and 19 percent strongly disagreeing with idea that they do not perceive a risk. This was followed by *Additional specialised staff for government needs* with 70 percent disagreeing and 30 percent strongly disagreeing, all respondents also perceived a risk for *Dynamic / flexible SLA* with 63 percent disagreeing and the remainder strongly disagreeing. Finally, there was also a perception of

risk for *Meet government specific requirements* with 58 percent disagreeing and 36 percent strongly disagreeing (see Figure 5-18).

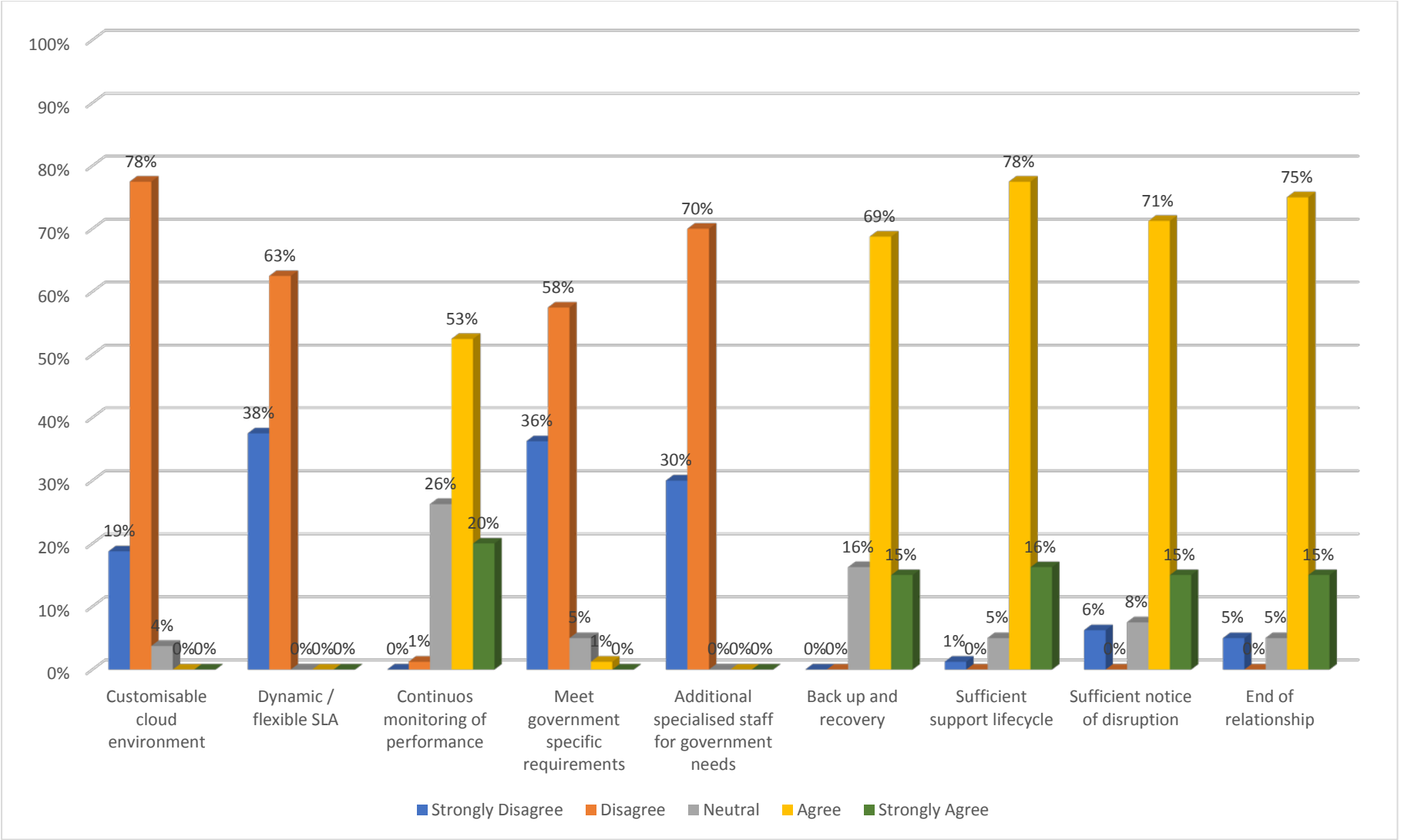
Although there was initially a low level of perceived risk for performance and offering generally, looking at the sub cloud factors it has been shown that there is significant perception of risk in some of the sub cloud factors of performance and offering which include those areas which are related to the particular needs of government, a customisable cloud environment and a Dynamic SLA have been shown to be of importance to government, as well as the need for specialised staff to cater for government needs.

Despite the negative perception of risk for the aforementioned cloud factors, there were some sub cloud factors where there was a positive perception of risk, they included *End of relationship* with 75 percent agreeing and 15 percent strongly agreeing, *Sufficient notice of disruption* with 71 percent agreeing and 15 percent strongly agreeing, *Backup and recovery* with 69 percent and 15 percent respectively, and finally, the least perception of a risk was found for *Sufficient support lifecycle* with 78 percent agreeing and 15 percent strongly agreeing that they do not perceive a risk.

As with the results for the other cloud factors, for the sub cloud factors that are generally a condition for most customers of the public cloud there is a much lower perception of risk. These cloud factors are general and are expected as part of a standard service provision.

In keeping with the other cloud factors, although there was certainty about whether or not a risk was perceived for the cloud factor, there was more certainty about how the government felt about individual sub cloud factors.

Figure 5-18: Risk and Sub Cloud Factors of Performance and Offering



5.4.1.12 Risk with other relationship factors (Performance and Offering) (Spearman correlation)

Table 5-10: Risk with other relationship factors (performance and offering) (Spearman correlation)

Relationship factors	Trust	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Risk	weak 0.380**	NC	moderate 0.485**	NC	NC	NC	NC	NC

For performance and offering, there were only correlations found between risk and trust which was weak and risk and CSP understands requirements which was found to be moderate. For the latter the sub cloud factors of performance and offering *Customisable cloud environment, Dynamic / flexible SLA, Continuous monitoring of performance, Additional specialised staff for government needs, Sufficient support lifecycle, End of relationship*, all of which showed positive weak Spearman correlations.

Although there was no statistically significant correlation between risk and collaboration in relation to performance and offering, the sub cloud factor *Continuous monitoring of performance* showed a strong correlation (0.634** Spearman). This means that although generally there is no link between the perception of risk and collaboration, there was a perceived ability to collaborate for this sub cloud factor.

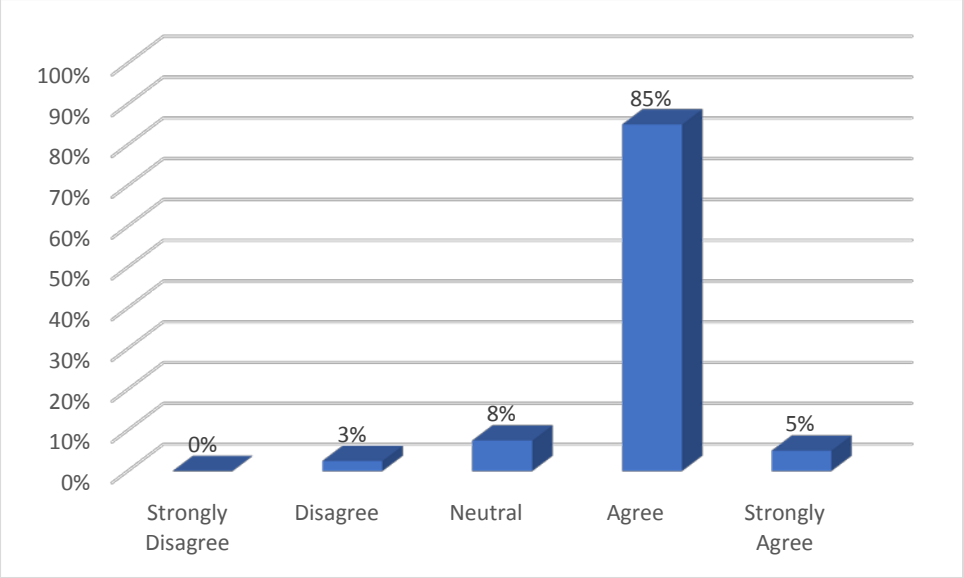
Although there was no correlation between risk and effectively communicate, the sub cloud factor *Continuous monitoring of performance* received a strong positive correlation (0.634** Spearman) as with previous results. Therefore, for this sub cloud factor, which always receives a very low perception of risk, there is often an associated high perception of the ability to effectively communicate.

5.5 Collaboration Domain – Relationship Factor

5.5.1 Collaboration

Respondents mostly agreed with the idea that they could collaborate with the CSP, this was evidenced by 90 percent agreement with this idea (see Figure 5-19).

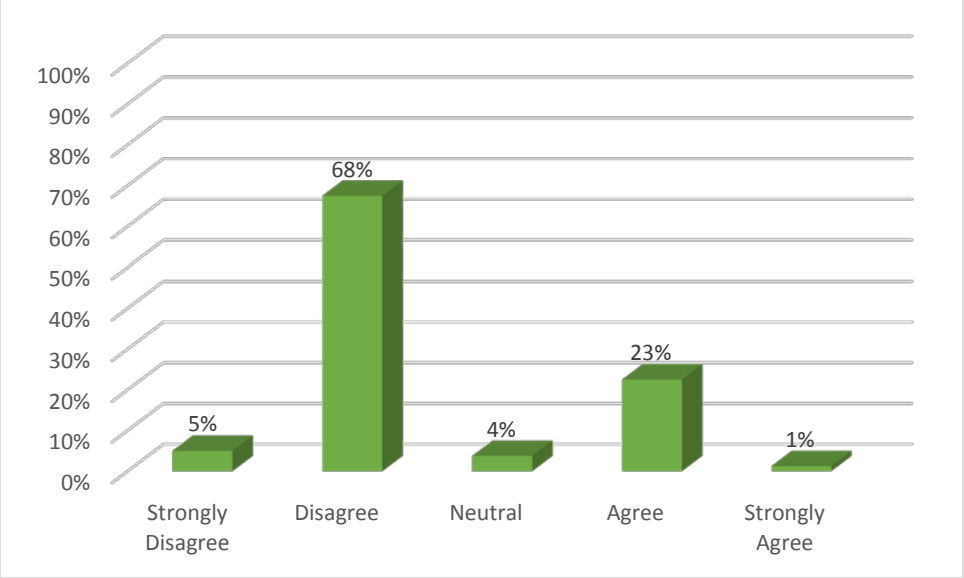
Figure 5-19: Collaboration General



5.5.1.1 Collaboration and Governance

Although the respondents largely agreed that they could collaborate with the CSP, where the respondents were asked about collaboration for governance generally they mostly disagreed with this idea. The results showed that 68 percent disagreed and 5 percent strongly disagreed with this idea, however, there was a significant amount, 24 percent, who agreed with this idea (see Figure 5-20).

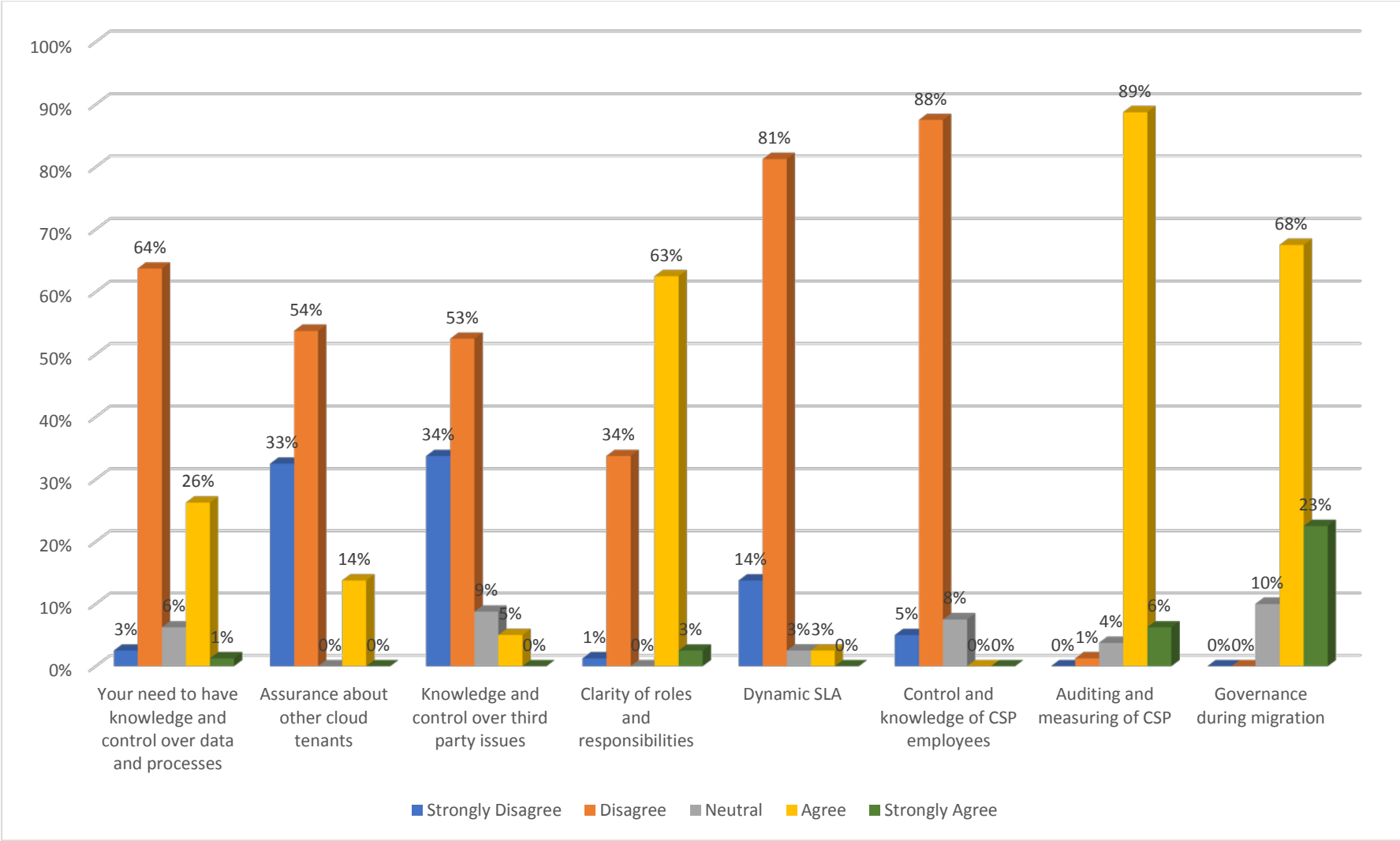
Figure 5-20: Collaboration for Governance (Q12A)



5.5.1.2 Collaboration and Sub Cloud Factors of Governance

The opinion that respondents disagreed that that they could collaborate on governance continues where they are asked about collaboration and the sub cloud factors of governance. There was disagreement for collaboration for *Knowledge and control of CSP employees* with 88 percent disagreeing, *Dynamic SLA* with 81 percent disagreeing, *Knowledge and control over third party issues* with 53 percent disagreeing and a significant 34 percent strongly disagreeing, similar results were found for *Assurance about other cloud tenants* at 54 percent and 33 percent respectively, finally the *Need to have knowledge and control over data and processes* with 64 percent disagreeing. Therefore, these results show that government respondents feel that they cannot collaborate on these areas of governance and in consideration of the fact that these are areas that are essential for government in the public cloud this would explain an overall reluctance to adopt the cloud (see Figure 5-21).

Figure 5-21: Collaboration and Sub Cloud Factors of Governance



Where there was a positive perception that the government respondents could collaborate with the CSP was for *Auditing and measuring of CSP* with 89 percent, *Governance during migration* at 68 percent with 23 percent strongly agreeing, there was also some agreement for *Clarity of roles and responsibilities* at 63 percent agreeing that they could collaborate, however, it is important to note that 34 percent did disagree with this idea (see Figure 5-21).

5.5.1.3 Collaboration with other relationship factors (Governance) (Spearman correlation)

Table 5-11: Collaboration with other relationship factors (governance) (Spearman correlation)

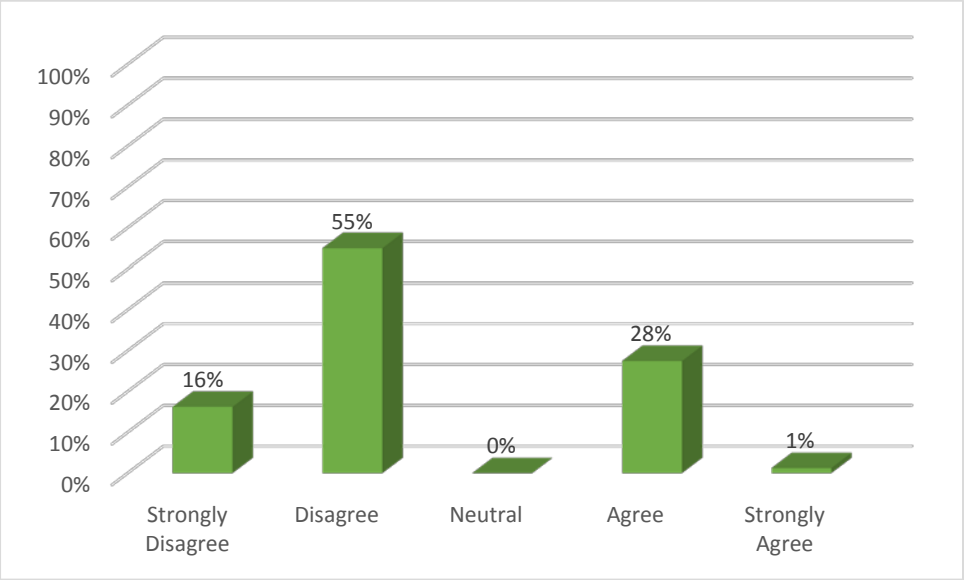
Relationship factors	Trust	Risk	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Effectively collaborate with CSP	moderate 0.595**	weak 0.300**	NC	weak 0.338**	strong 0.707**	moderate 0.433**	weak 0.362**	moderate 0.476**

A strong correlation was found between the perceived ability to collaborate with the CSP for governance and the ability to negotiate for governance. Moderate correlations were found between the ability to collaborate with the CSP for governance and trust, effectively communicate and perception of a positive reputation for governance (see Table 5-11).

5.5.1.4 Collaboration and Compliance

The majority of the respondents, 55 percent disagreeing and 16 percent strongly disagreeing, that they could collaborate with the CSP about compliance, however, a significant 28 percent did agree that they could collaborate on compliance (see Figure 5-22).

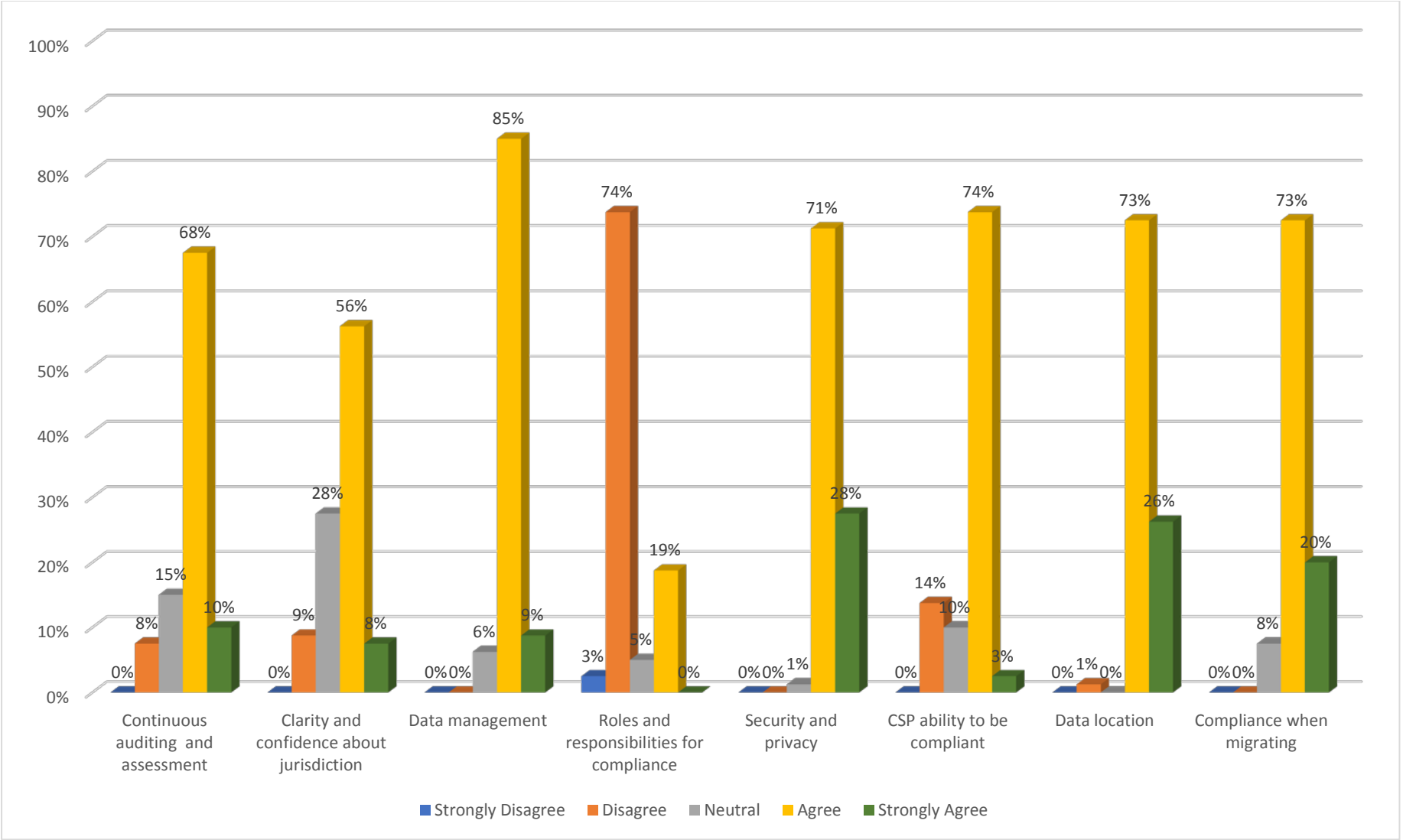
Figure 5-22: Collaborate for Compliance (Q12B)



5.5.1.5 Collaboration and Sub Cloud Factors of Compliance

Despite the fact that there was a high level of disagreement with the idea that the government respondents could collaborate on compliance, when asked about the sub cloud factors of compliance there was a high level of agreement that they could collaborate for all of the sub cloud factors except one. Where there was a disagreement it was for the sub cloud factor of *Roles and responsibilities for compliance* where 74 percent disagreed (see Figure 5-23).

Figure 5-23: Collaboration and Sub Cloud Factors of Compliance



5.5.1.6 Collaboration with other relationship factors (Compliance) (Spearman correlation)

Table 5-12: Collaboration with other relationship factors (compliance) (Spearman correlation)

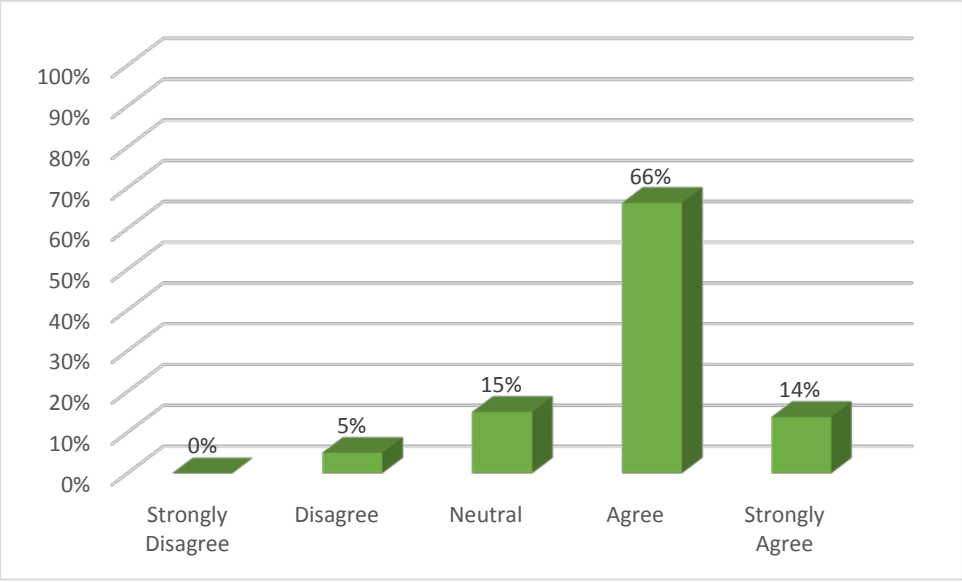
Relationship factors	Trust	Risk	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Effectively collaborate with CSP	strong 0.662**	moderate 0.426**	NC	moderate 0.463**	moderate 0.426**	NC	moderate 0.554**	strong 0.615**

In reference to the perceived ability of the government to collaborate for compliance, strong correlations were found for trust in compliance and perceived positive reputation (see Table 5-12). This means that because there was a high level of disagreement with the idea that the government could effectively collaborate for compliance, there was an associated strong mistrust and perception of a negative reputation for compliance.

5.5.1.7 Collaborate and Security and Privacy

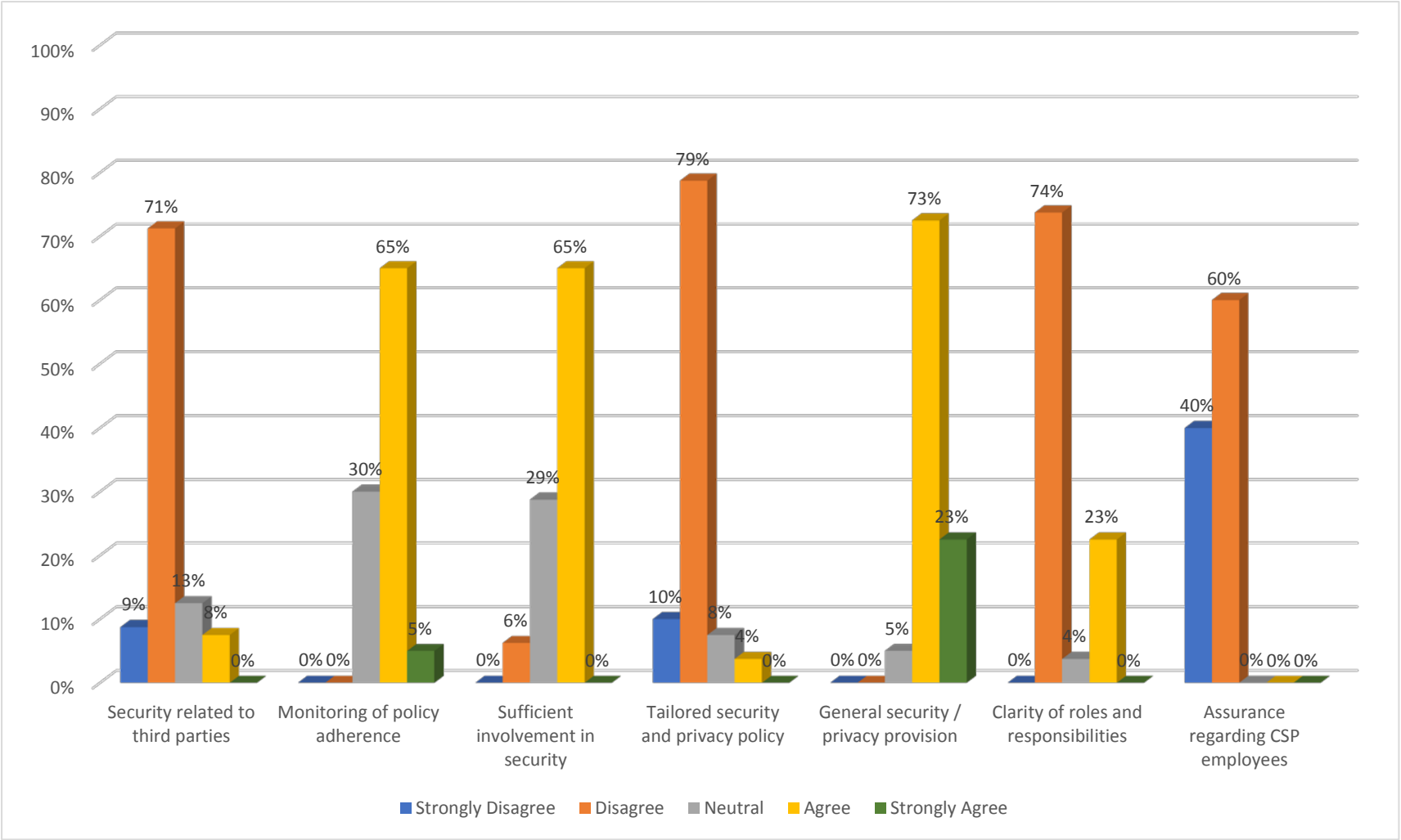
Security and privacy was a cloud factor that the government respondents felt they could collaborate for with the CSP. This was evidenced by the fact that 66 percent agreed and 14 percent strongly agreed with this idea and only 5 percent disagreed, there were a significant number, 15 percent, responded neutral (see Figure 5-24).

Figure 5-24: Collaborate for Security and Privacy (Q12C)



5.5.1.8 Collaboration and Sub Cloud Factors of Security and Privacy

Figure 5-25: Collaboration and Sub Cloud Factors of Security and Privacy



As was found to be the case for other relationship factors where the government respondents were asked about the associated sub cloud factors, there was a mixture of opinions. Moreover, the results again show that where the government respondents have less confidence in a particular relationship factor regarding the sub cloud factors, is in the areas that would be of particular concern to a government considering the public cloud. Specifically, there was a high level of disagreement with *Tailored security and privacy policy* with 79 percent disagreeing, *Clarity of roles and responsibilities* with 74 percent disagreement and *Security related to third parties* with 71 percent disagreement. The highest level of disagreement was for *Assurance regarding CSP employees* whereby 60 percent disagreed and 40 percent strongly disagreed (see Figure 5.25). There were high levels of agreement for *General security / privacy provision* 73 percent agreeing and 23 percent strongly agreeing, followed by *Sufficient involvement in security* at 65 percent agreement, although it is important to note that 29 percent gave their answer as neutral. This was similar to *Monitoring of policy adherence* with 65 percent agreeing and 30 percent giving their answer as neutral (see Figure 5-25).

5.5.1.9 Collaboration with other relationship factors (Security and Privacy) (Spearman correlation)

Table 5-13: Collaboration with other relationship factors (security and privacy) (Spearman correlation)

Relationship factors	Trust	Risk	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Effectively collaborate with CSP	weak 0.284*	NC	weak 0.352**	moderate 0.535**	moderate 0.514**	moderate 0.509**	weak 0.283*	weak 0.290**

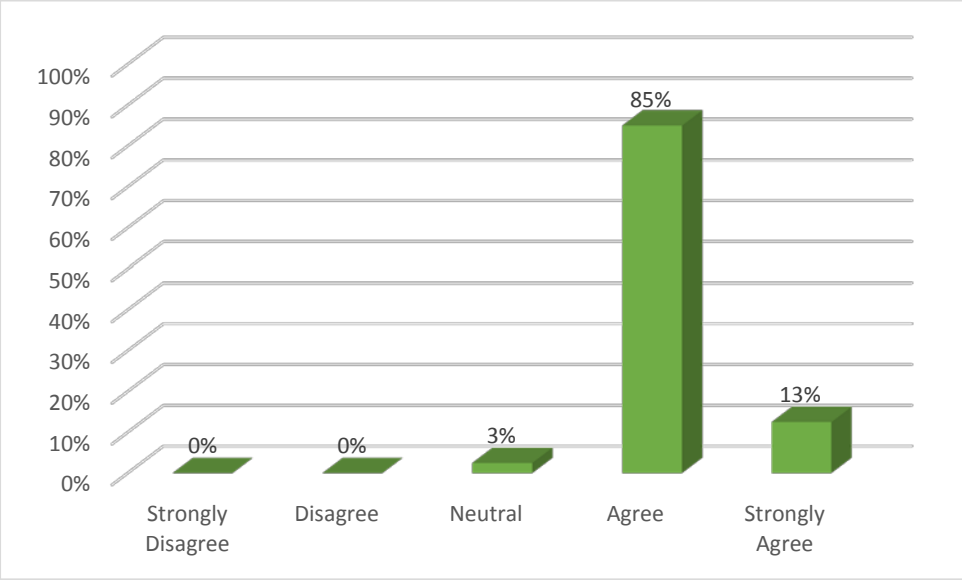
Between the perception of being able to effectively collaborate with the CSP for security and privacy and other relationship factors, there were three moderate correlations with other relationship factors which included CSP understands requirements, ability to negotiate, and effectively communicate. Because there is a high level of agreement with the idea that the government can effectively collaborate for security and privacy there was an associated positive perception that the government had the ability to negotiate and effectively

communicate for security and privacy as well as the perception that the CSP understood these requirements.

5.5.1.10 Collaboration and Performance and Offering

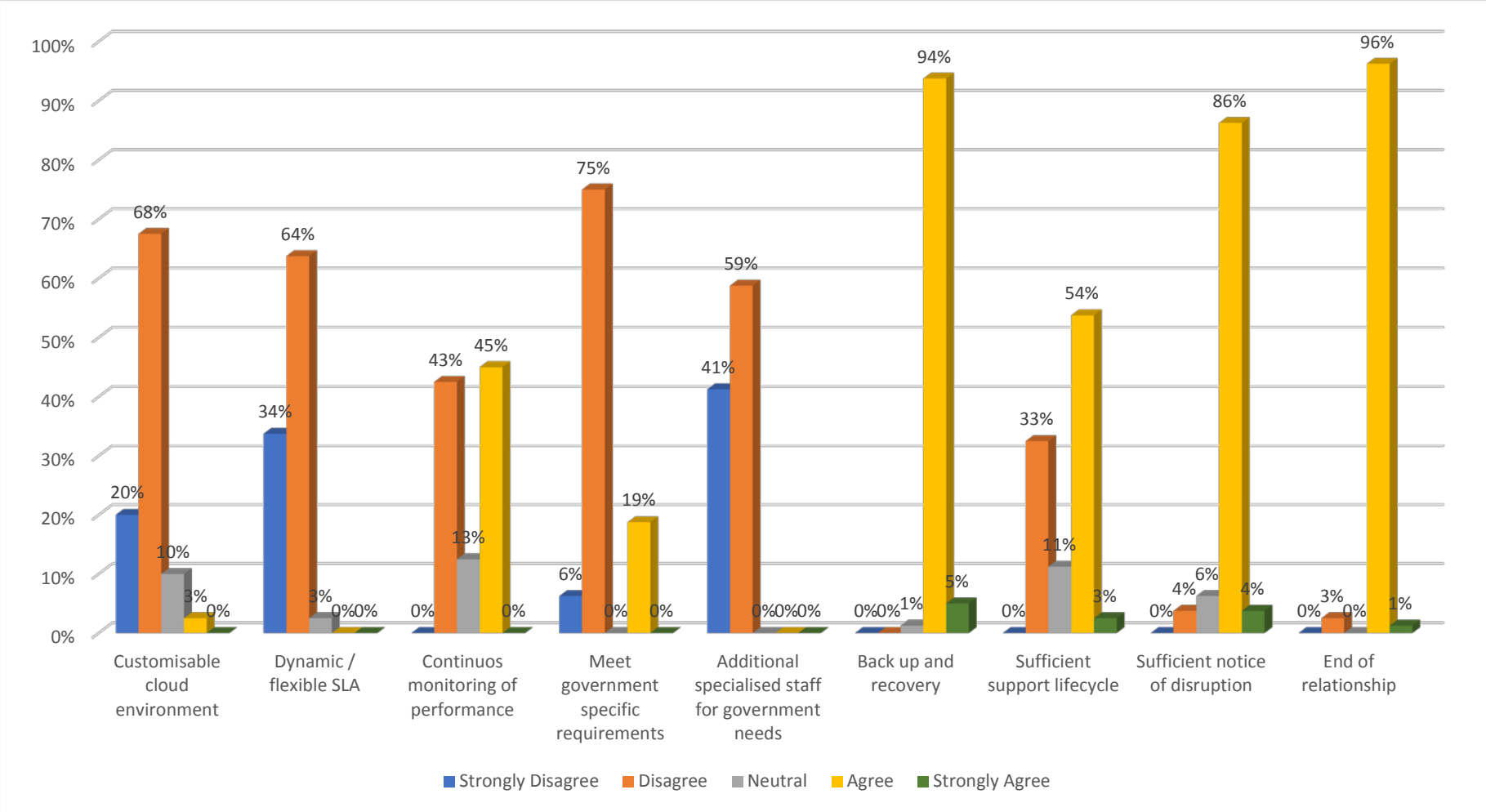
Almost all of the government respondents agreed with the idea that they could collaborate with their CSP in relation to performance an offering. This was clearly evidenced by the fact that 85 percent agreed and 13 percent strongly agreed with this idea, moreover, none of the respondents disagreed that they could collaborate on performance and offering (see Figure 5-26).

Figure 5-26: Collaborate on Performance and Offering (Q12D)



5.5.1.11 Collaboration and Sub Cloud Factors of Performance and Offering

Figure 5-27: Collaboration and Sub Cloud Factors of Performance and Offering



Where the respondents were asked about the sub cloud factors of performance and offering the results were contrasted with performance and offering generally. Again, as with other results shown in this study there was a high level of disagreement with those sub cloud factors that would be a particular concern to government. This high level of disagreement was shown to be evident for *Additional specialised staff for government needs* with all of the respondents disagreeing or strongly disagreeing, *Meet government specific requirements* with 75 percent disagreement and *Customisable cloud environment* with 68 percent disagreement and 20 percent strongly disagreeing. There was also a strong level of disagreement with the idea that the government respondents could collaborate on the issue of a *Dynamic / flexible SLA* with 64 percent disagreeing and 34 percent strongly disagreeing with this idea (see Figure 5-27)

5.5.1.12 Collaboration with other relationship factors (Performance and Offering) (Spearman correlation)

Table 5-14: Collaboration with other relationship factors (performance and offering) (Spearman correlation)

Relationship factors	Trust	Risk	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Ability to negotiate (negotiation)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Effectively collaborate with CSP	weak 0.271*	NC	weak 0.328**	NC	weak 0.250*	moderate 0.510**	NC	weak 0.386**

There was little correlation between the perceived ability to effectively collaborate with the CSP and other relationship factors for performance and offering. The results show that the perceived ability to collaborate for performance and offering was moderately linked to the ability to effectively communicate for the same cloud factor (see Table 5-14). Therefore, the ability to collaborate for performance and offering has very little bearing on other relationship factors.

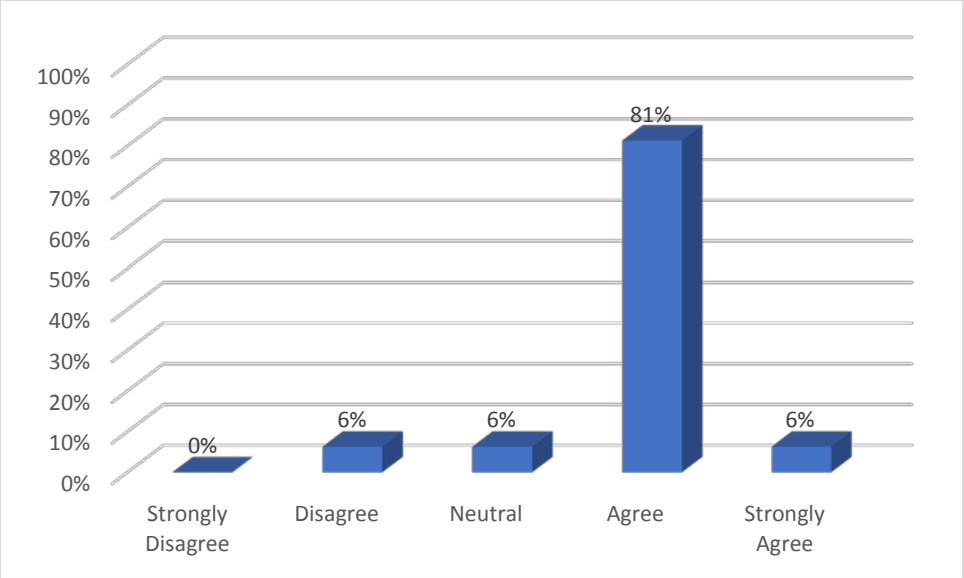
5.6 Negotiation - Relationship Factor

Negotiation as a relationship factor is analysed against the various cloud and sub cloud factors. Here negotiation is addressed generally and in subsequent sections different aspects of negotiation are addressed.

5.6.1 Negotiation

There was a very high level of agreement with the idea that the government respondents could negotiate with their CSP. This was evidenced by 81 percent agreeing and 6 percent strongly agreeing with this idea, moreover, only 6 percent disagreed with this idea (see Figure 5-29).

Figure 5-28: Negotiation

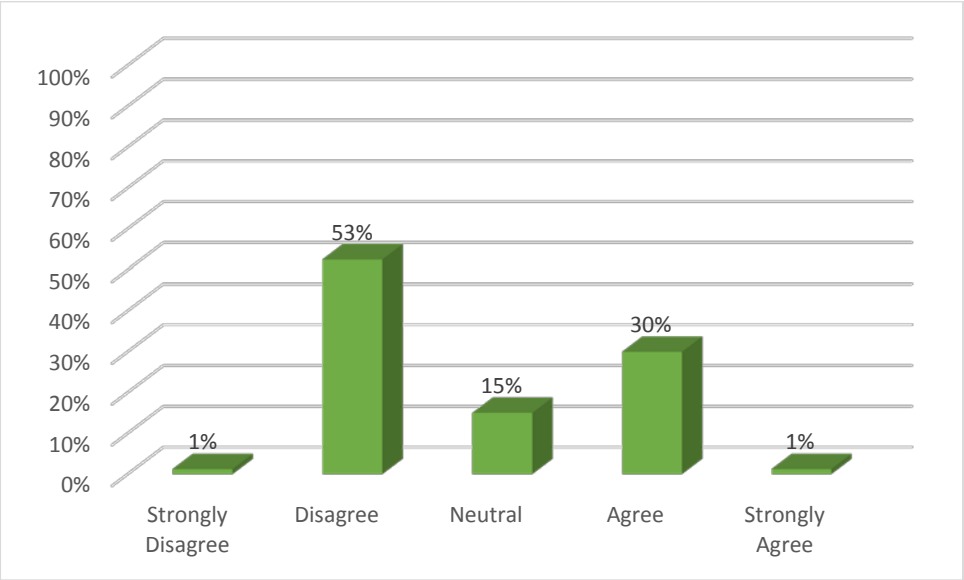


5.6.2 Negotiation with Cloud Factors and Sub Cloud Factors

Firstly, negotiation with each cloud factor is addressed followed by sub cloud factors, thereafter, negotiation with other relationship factors.

5.6.2.1 *Negotiation and Governance*

Figure 5-29: Negotiation Q10A Governance

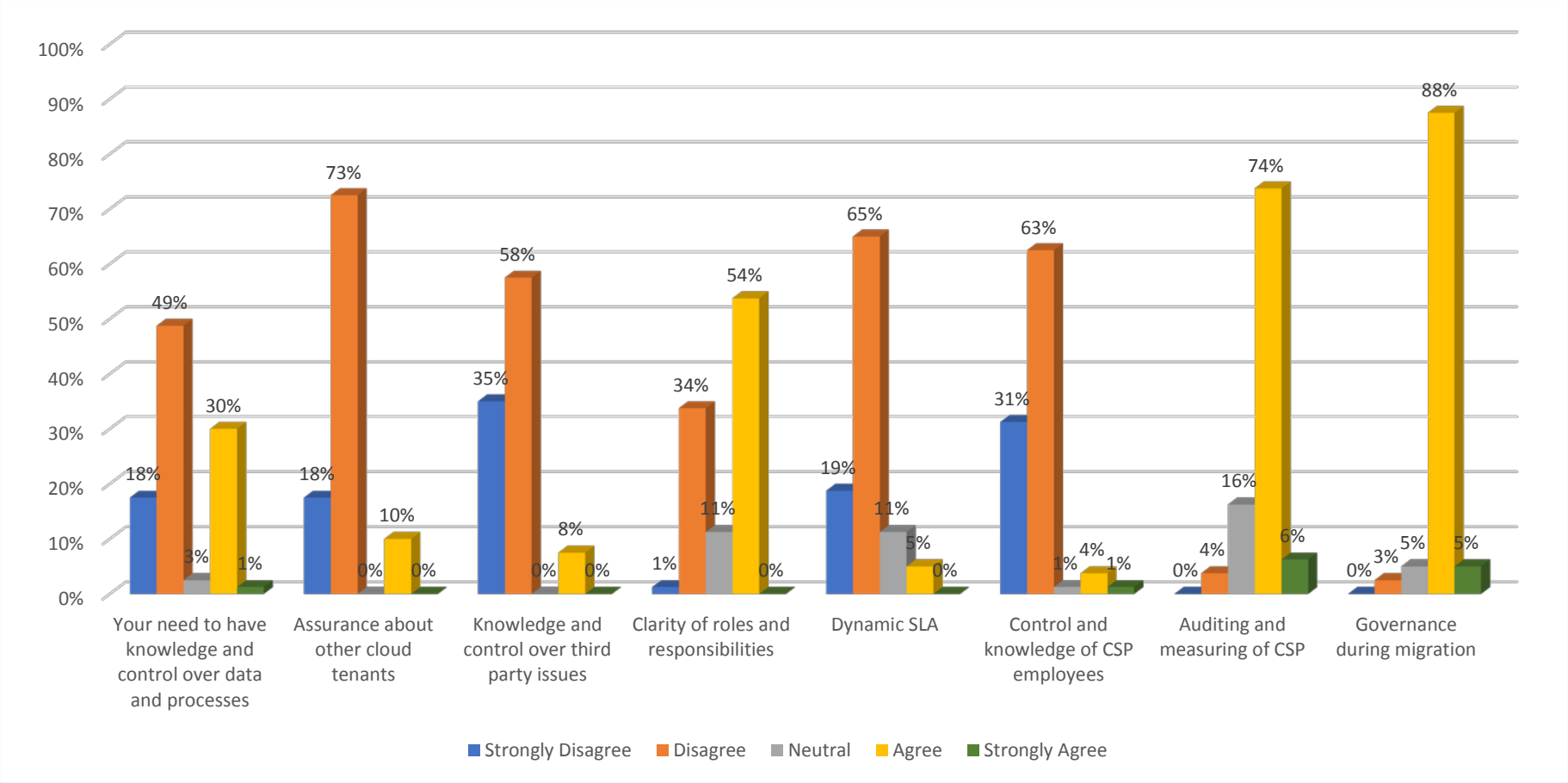


A majority of the respondents disagreed with the idea that they could negotiate with their CSP in relation to governance. This was evidenced by the results which show that 53 percent disagreed with the idea with 1 percent strongly disagreeing. However, it is fair to say that a significant number, 30 percent and 1 percent agreed and strongly agreed, respectively, that they could negotiate governance with their CSP. Moreover, 15 percent gave the response as neutral meaning they neither agreed or disagreed with this idea (see Figure 5-30).

5.6.2.2 *Negotiation and Sub Cloud Factors of Governance*

The results for the sub cloud factors of governance also showed a high level of disagreement that the government respondents could negotiate with the CSP. There were strong levels of disagreement in particular for *Control and knowledge of CSP employees* with 63 percent disagreeing and 31 percent disagreeing, *Dynamic SLA* with 65 percent and 19 percent, *Knowledge and control over third party issues* with 58 percent and 35 percent, *Assurance about other cloud tenants* at 73 percent and 18 percent, and *Need to have knowledge and control over data and processes* at 49 percent and 18 percent, all respectively for disagree and strongly disagree (see Figure 5-31).

Figure 5-30: Negotiation and Sub Cloud Factors of Governance



In line with the idea that the respondents did not feel they could negotiate with their CSP about governance generally as a cloud factor, there were only two sub cloud factors where the government respondents felt that they could negotiate, these were *Governance during migration* 88 percent agreeing and *Auditing and measuring of CSP* with 74 percent agreeing and 6 percent strongly agreeing.

Where there is a commonality between these results and the results for the relationship factors of trust and risk is that where there is a level of confidence, in this case confidence that the government can negotiate in relation to the sub cloud factors of *Governance during migration* and *Auditing and measuring of CSP*, these are for sub cloud factors that are general and would be expected in a standard SLA, whereas the other sub cloud factors are those that would be of a particular concern to government.

5.6.2.3 Negotiation with other relationship factors (governance) (Spearman correlation)

Table 5-15: Negotiation with other relationship factors (governance) (Spearman correlation)

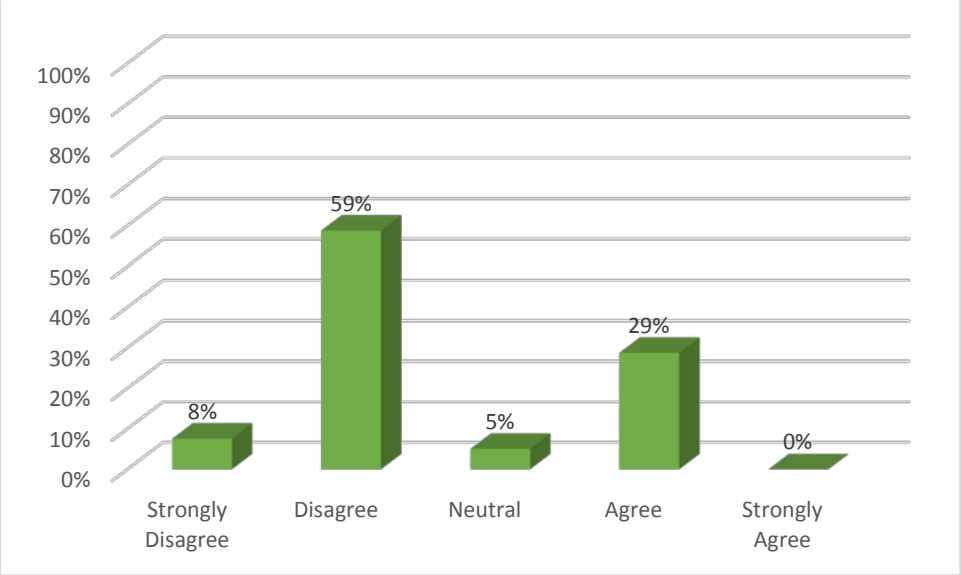
Relationship factors	Trust	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Risk	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Ability to negotiate (negotiation)	moderate 0.508**	NC	moderate 0.430**	Moderate 0.423**	Strong 0.707**	moderate 0.562**	moderate 0.415**	Moderate 0.527**

Overall, for governance there were significant links between the ability to negotiate and the other relationship factors, with the exception of effectively specify requirements. Particularly, there was a strong positive correlation between the ability to negotiate for governance and the ability to collaborate for governance, this was evidenced by a Spearman correlation of 0.707 (**).

5.6.2.4 Negotiation and Compliance

There was also a high level of disagreement with the idea that the government respondents could negotiate for compliance generally as a cloud factor. In total 59 percent of the respondents disagreed with this idea and 8 percent strongly disagreed. However, there was a significant 29 percent who did agree (see Figure 5-32).

Figure 5-31: Negotiation and Compliance

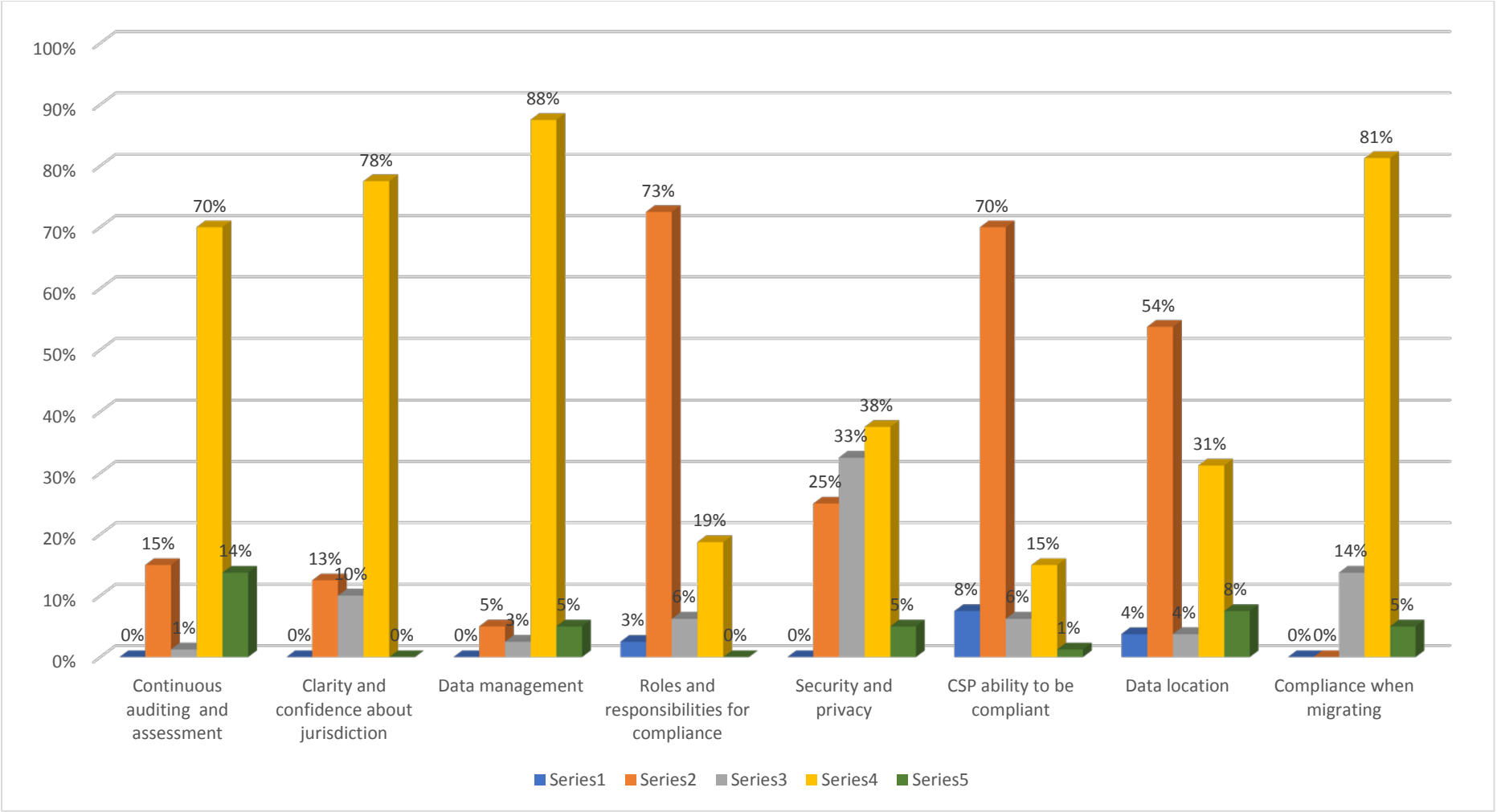


5.6.2.5 Negotiation and Sub Cloud Factors of Compliance

Despite the fact that the government respondents mostly felt that they disagreed with the idea that they could negotiate in regard to compliance, they did feel that they can negotiate with the CSP for most of the sub cloud factors for compliance. The most agreement was found for *Data management* with 88 percent, followed by *Compliance when migrating* at 81 percent, *Clarity and confidence about jurisdiction* at 78 percent and *Continuous auditing and assessment* at 70 percent (see Figure 5-33). Therefore, the government respondents felt that they were confident to negotiate the issue of jurisdiction.

The initial response for compliance as a cloud factor was shown to be different to the responses for the sub cloud factors, again this is a recurring theme that when asked about sub cloud factors in particular the government were more certain in their responses.

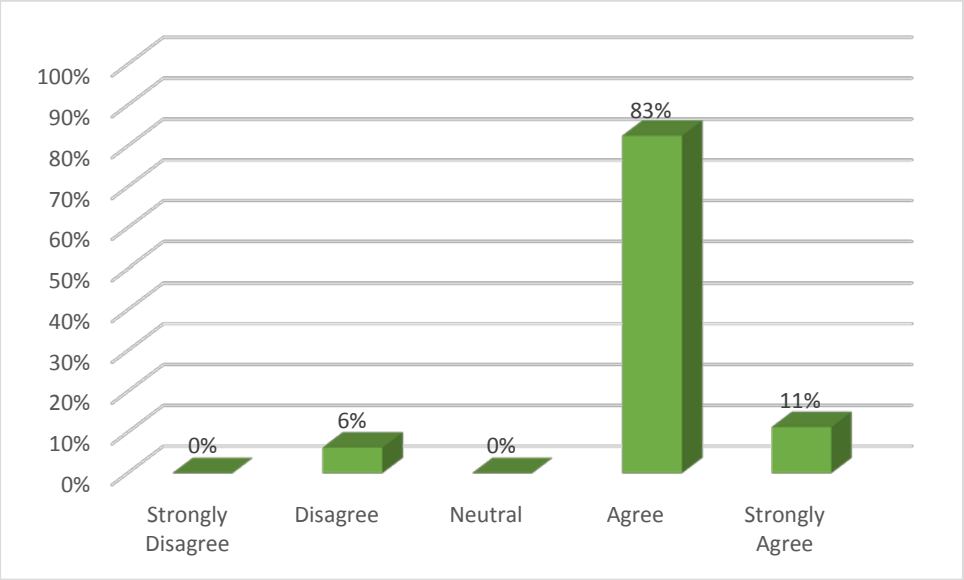
Figure 5-32: Negotiation and Sub Cloud Factors of Compliance



5.6.2.6 Negotiation and Security and Privacy

There was a high level of agreement with the idea that the government respondents could negotiate security and privacy with 83 percent agreeing and 11 percent strongly agreeing with this idea, and only 6 percent in disagreement (see Figure 5-34).

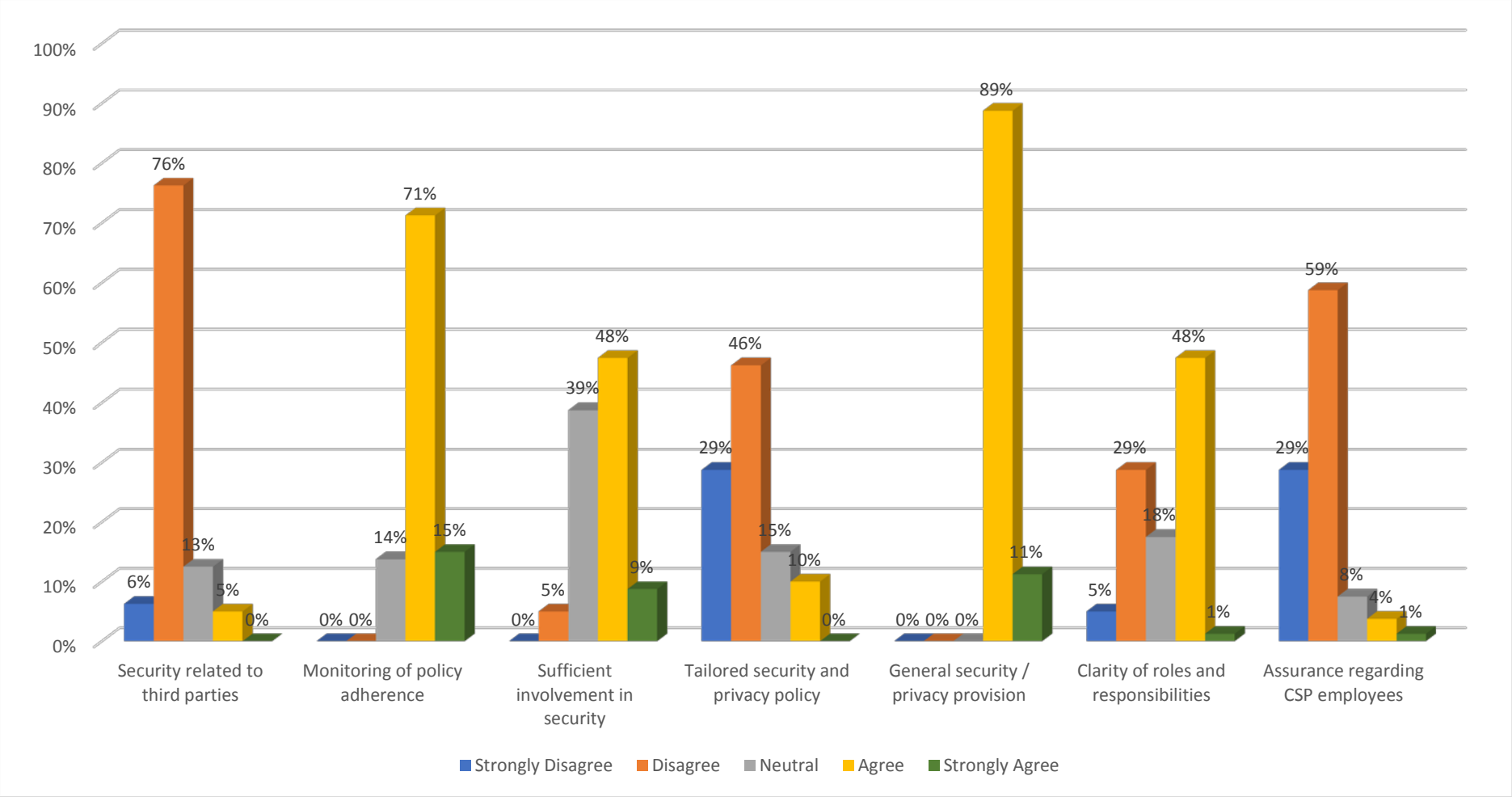
Figure 5-33: Negotiation and Security and Privacy



5.6.2.7 Negotiation and Sub Cloud Factors of Security and Privacy

There were mixed opinions when the respondents were questioned about the sub cloud factors of security and privacy. There was very strong agreement with the idea that the government could negotiate *General security / privacy provision* with 89 percent agreement and 11 percent strongly agreeing with this idea, this was followed by *Monitoring of policy adherence* with 71 percent in agreement and 15 percent strongly agreeing, there was also agreement that the respondents could negotiate for *Clarity of roles and responsibilities* and *Sufficient involvement in security* (see Figure 5-35).

Figure 5-34: Negotiation Q9 and Sub Cloud Factors of Security and Privacy



As with the other relationship factors and the associated sub cloud factors there was disagreement in the areas that can be considered to be a particular concern to government. *Security related to third parties* received the highest level of disagreement at 76 percent, followed by *Assurance regarding CSP employees* with 59 percent disagreeing and a significant 29 percent strongly disagreeing, and finally, *Tailored security and privacy policy* with 46 percent disagreement and 29 percent strongly disagreeing. Concern about third parties which include those who provide the cloud infrastructure is a concern for government because they need to ensure that they are compliant and protect citizen data.

5.6.2.8 Negotiation with other relationship factors (Security and Privacy) (Spearman correlation)

Table 5-16: Negotiation with other relartionship factors (Security and Privacy) (Spearman correlation)

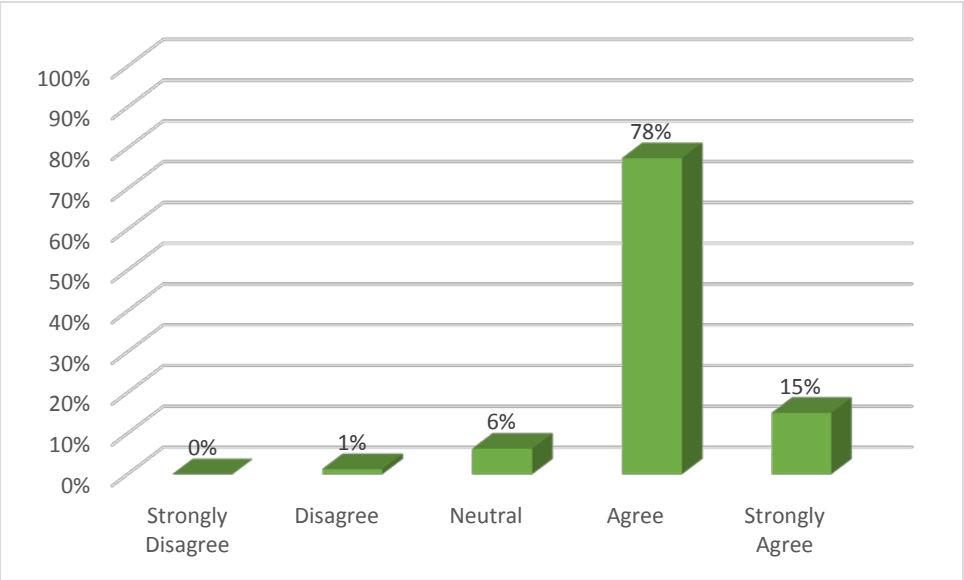
Relationship factors	Trust	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Risk	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Ability to negotiate (negotiation)	weak 0.310**	Weak 0.324**	Weak 0.380**	NC	moderate 0.514**	moderate 0.403**	moderate 0.418**	moderate 0.500**

There were positive and moderate correlations between the ability to specify requirements for security and privacy and effectively collaborate, effectively communicate and perceived a positive reputation for security and privacy. Positive but weak correlations were found between ability to negotiate and trust, effectively specify requirements and CSP understands requirements, no correlation was found between ability to negotiate for security and privacy and trust in security and privacy (see Table 5-16). The latter finding shows that while it may be assumed that trust in a particular cloud factor may have a positive effect on other relationship factors such as the ability to collaborate or communication, in this case this is not true for the ability to specify requirements. Having enough information, perceiving a positive reputation, the ability to communicate and collaborate are more likely to have an impact on the ability to negotiate for security and privacy. Interestingly, the other two aspects of negotiation were found to have a much weaker link on the ability to negotiate.

5.6.2.9 Negotiation and Performance and Offering

There was also a high level of agreement with the idea that the government respondents could negotiate with their CSP about performance and offering, this was evidenced by 78 percent of the respondents agreeing with this idea and 15 percent strongly agreeing, in fact only 1 percent disagreed (see Figure 5-36).

Figure 5-35: Negotiation and Performance and Offering



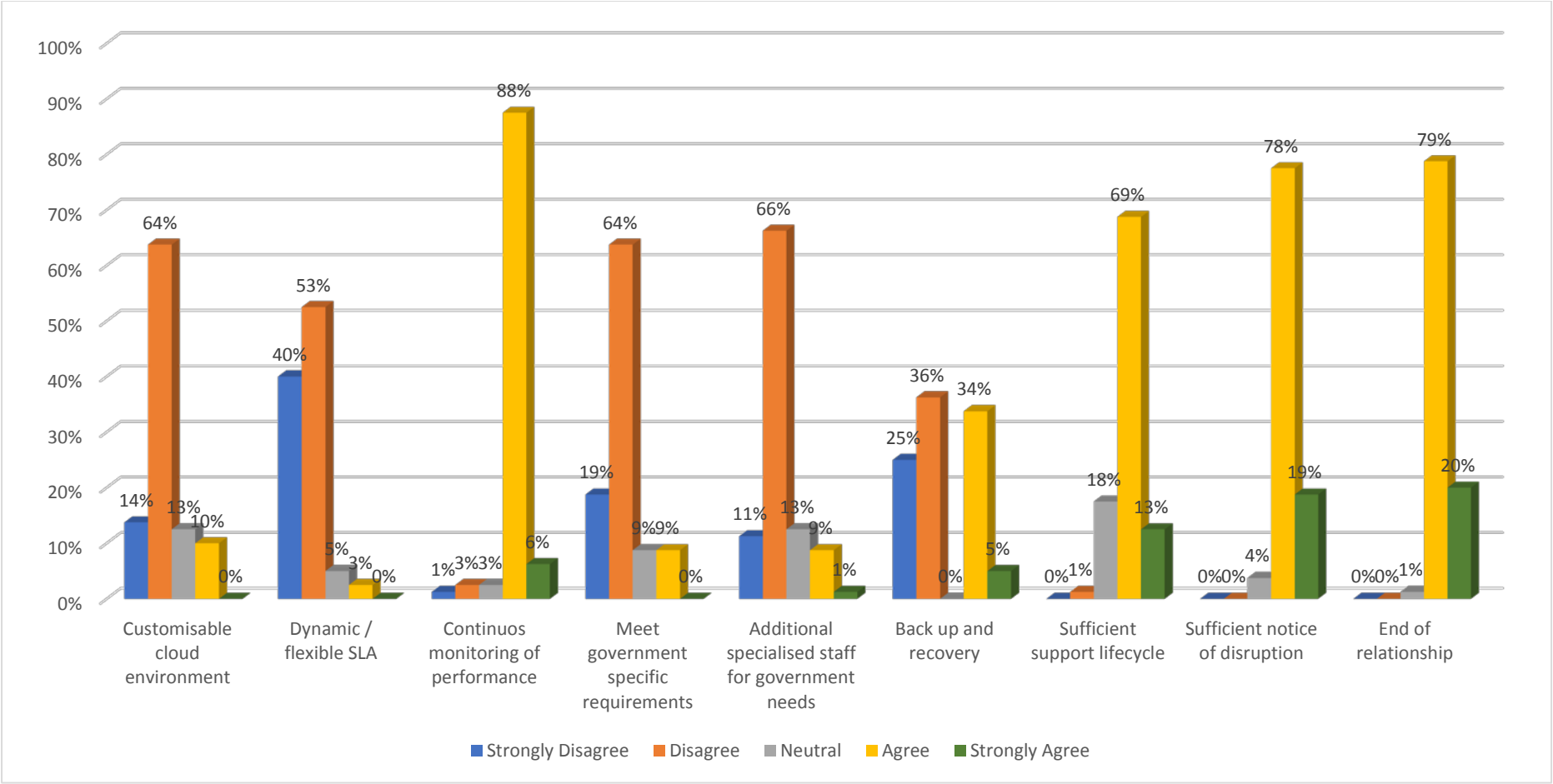
5.6.2.10 Negotiation and Sub Cloud Factors of Performance and Offering

Again, there were mixed results when the respondents were questioned about the sub cloud factors of performance and offering. Although the respondents agreed that they could negotiate performance and offering generally, there was disagreement of 66 percent with *Additional specialised staff for government needs* (see Figure 5-37). This would suggest that government may feel reluctant to adopt the public cloud because they feel they cannot negotiate specialised staff within the CSP that can look after government needs. Likewise, there was also a high level of disagreement that the government could negotiate for government requirements to be met with 64 percent disagreeing and a significant 19 percent strongly disagreeing with this idea. There was also a high level of disagreement that the government could negotiate a *Customisable cloud environment* with 64 percent disagreeing and 14 percent strongly disagreeing, this is closely related to the idea of a Dynamic / flexible SLA whereby government can hope to achieve a tailored and flexible service in order to meet their complex and ever-changing needs. The level of disagreement with the idea that the

government could negotiate a *Dynamic / flexible SLA* was high with 53 percent disagreeing and 40 percent strongly disagreeing. Therefore, there is a lack of confidence that the government can negotiate for these performance and offering sub cloud factors that are of particular interest to government considering the public cloud, and therefore, this may be a contributing factor for reluctance to adopt the public cloud.

Where there was a particularly high level of confidence was for *Continuous monitoring and performance* with 88 percent of respondents agreeing that they could negotiate this area. This was followed by *End of relationship* with 79 percent agreeing and 20 percent strongly agreeing, *Sufficient notice of disruption* with 78 percent and 19 percent and *Sufficient support lifecycle* with 69 percent and 13 percent, all for agreement and strong agreement respectively (see Figure 5-37), all of which are standard SLA provisions.

Figure 5-36: Negotiation Q9 and Sub Cloud Factors of Performance and Offering



5.6.2.11 Negotiation with other relationship factors (Performance and Offering) (Spearman correlation)

Table 5-17: Negotiation with other relationship factors (performance and offering) (Spearman correlation)

Relationship factors	Trust	Effectively specify requirements (negotiation)	CSP understands requirements (negotiation)	Risk	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Ability to negotiate (negotiation)	weak 0238*	NC	Weak 0.247**	NC	weak 0.250*	weak 0.245*	NC	weak 0.338**

The overall link between the ability to negotiate for performance and offering and other relationship factors was weak at best. Therefore, the perceived ability to negotiate for performance and offering has no link to other relationship factors where performance and offering is concerned (see Table 5-17).

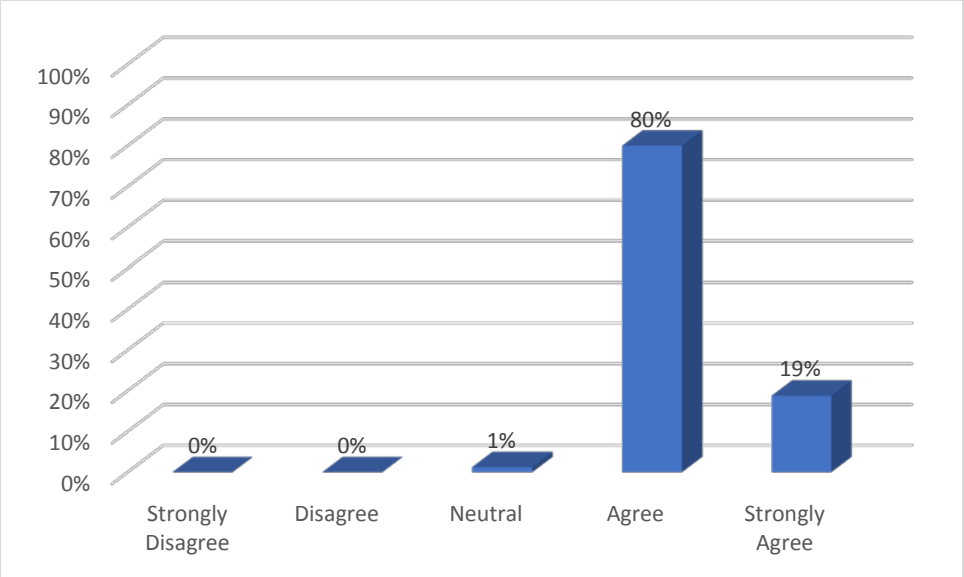
5.7 Negotiation (Specify Requirements) Relationship Factor

Negotiation, specifically the ability to specify requirements, as a relationship factor is analysed against the various cloud and sub cloud factors. Specifically, the perceived ability of the government to specify requirements for governance, compliance, security and privacy and performance and offering is analysed as well as an analysis of how the perceived ability to specify requirements is linked to other relationship factors.

5.7.1 Negotiation (Specify requirements)

There was a very high level of agreement with the idea that the government respondents could specify requirements with their CSP. This was evidenced by 80 percent agreeing and 19 percent strongly agreeing with this idea, and none disagreeing (see Figure 5-38).

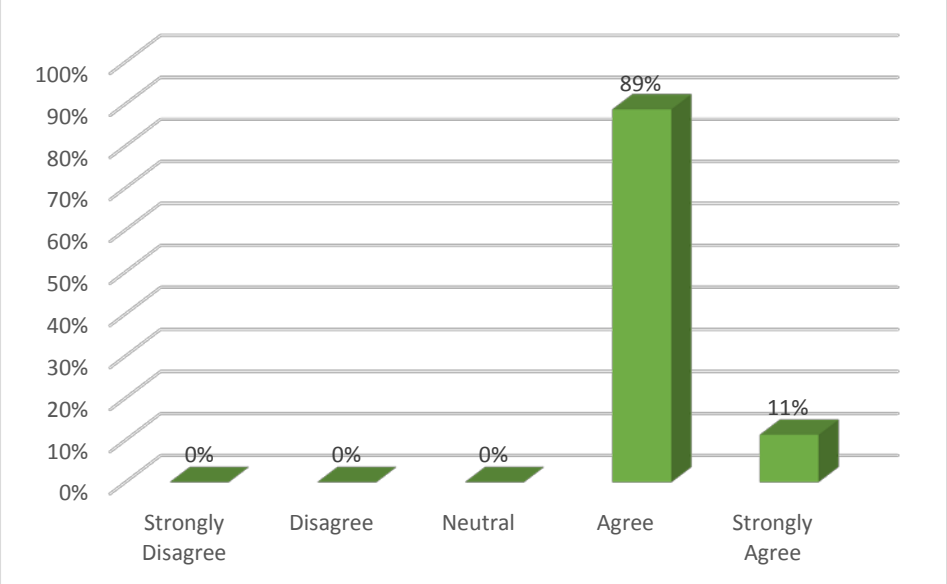
Figure 5-37: Negotiation – Specify Requirements



5.7.1.1 Negotiation (specify requirements) and Governance

The respondents agreed with the idea that they could specify requirements with their CSP in relation to governance. This was evidenced by the results which show that 89 percent agreed with the idea with 11 percent strongly agreeing (see Figure 5-39).

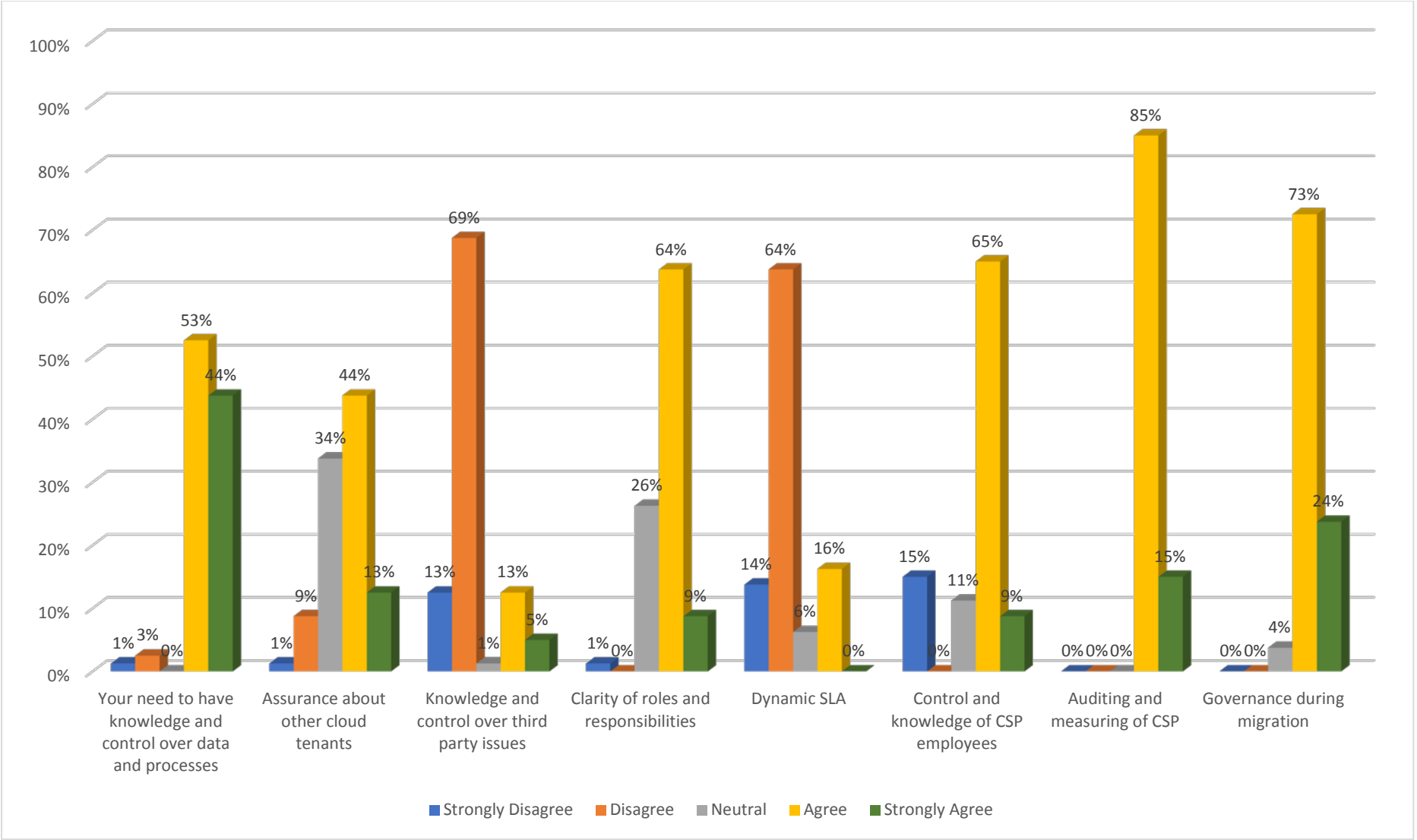
Figure 5-38: Negotiation (specify requirements) and Governance



5.7.1.2 Negotiation and Sub Cloud Factors of Governance

The results for the sub cloud factors of governance showed that there was a high level of disagreement the government respondents could negotiate with the CSP for two of the sub cloud factors of governance. There were strong levels of disagreement in particular for *Knowledge and control over third party issues* with 69 percent disagreeing, and *Dynamic SLA* with 64 percent disagreeing (see Figure 5-40).

Figure 5-39: Negotiation and Sub Cloud Factors of Governance



For previous relationship factors, there was often a difference between the level of agreement for the cloud factors and the level of agreement for the associated sub cloud factors. Often there is more certainty when sub cloud factors are addressed. In the case of negotiation where there is confidence to negotiate with the CSP, there is an associated confidence to negotiate for most cloud factors with the exception of *Knowledge and control over third party issues* and *Dynamic SLA*. Again, these are factors that are of particular concern and relevance to government, however, they were the only two sub cloud factors, there were sub cloud factors that would be of particular concern to government where positive responses were given, they included *assurance about other tenants* and *control and knowledge of CSP employees*. This was the only time that these government particular concerns received positive responses, it is important to note that specifying requirements is something that the government have a level of control over which could explain their perceived ability to specify for these requirements.

5.7.1.3 Negotiation (specify requirements) and Compliance

There was a high level of agreement with the idea that the government respondents could negotiate for compliance generally as a cloud factor. In total 71.3 percent of the respondents agreed and 25 percent strongly agreed with this idea see Table 5-18.

Table 5-18: Negotiation of Compliance

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0.0	0.0	0.0
	Disagree	0	0.0	0.0	0.0
	Neutral	3	3.8	3.8	3.8
	Agree	57	71.3	71.3	75.0
	Strongly Agree	20	25.0	25.0	100.0
	Total	80	100.0	100.0	

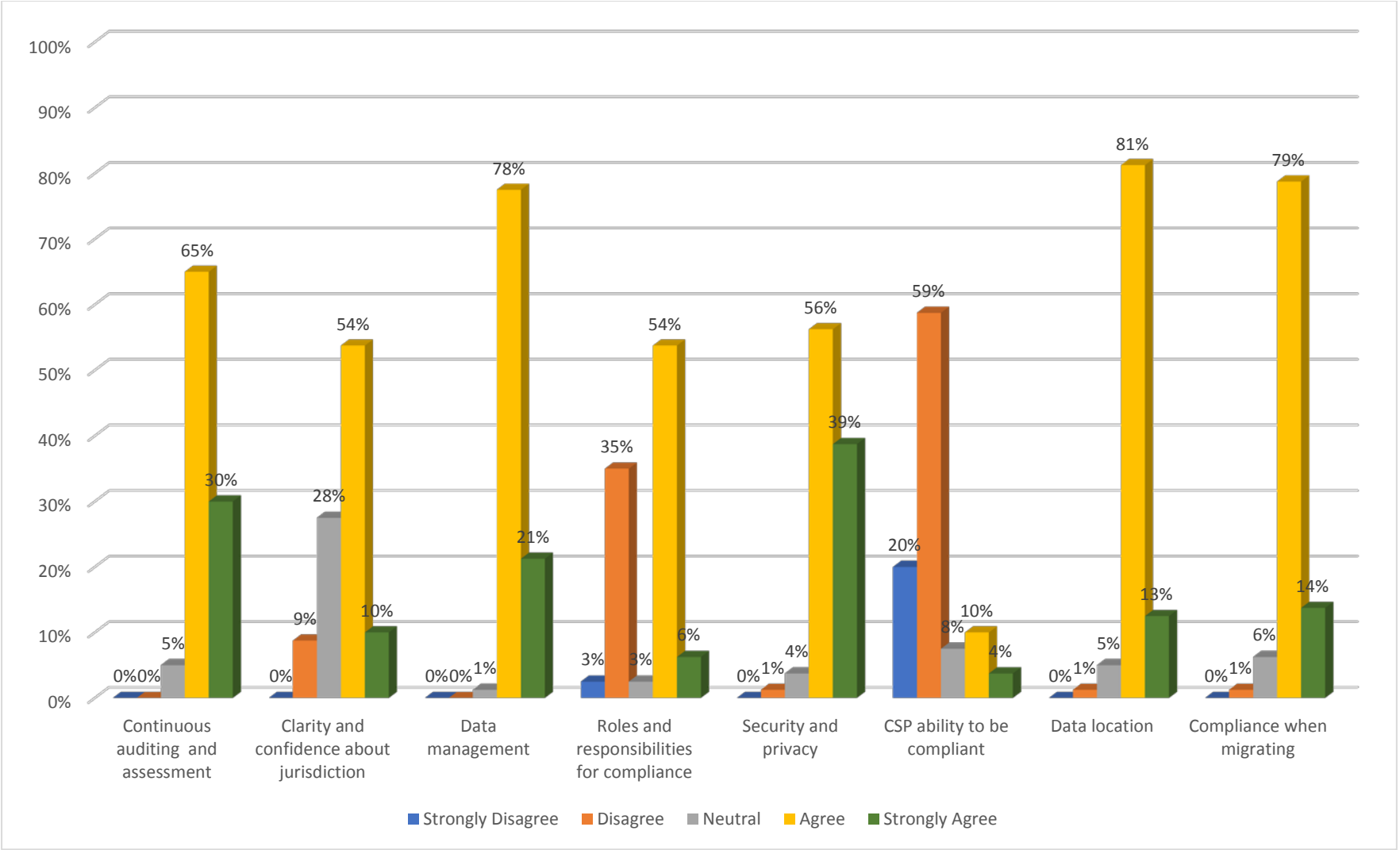
5.7.1.4 Negotiation (specify requirements) and Sub Cloud Factors of Compliance

Although the government respondents mostly felt that they disagreed with the idea that they could negotiate generally in regard to compliance, they felt that they can negotiate (specify requirements) with the CSP for most of the sub cloud factors for compliance. The most agreement was found for *Data management* with 78 percent agree and 21 percent strongly

agree, followed by *Compliance when migrating* at 79 percent and 14 percent, *Clarity and confidence about jurisdiction* at 54 percent and 10 percent and *Continuous auditing and assessment* at 65 percent and 30 percent, all respectively (see Figure 5-41).

The initial response for compliance as a cloud factor was shown to be different to the responses for the sub cloud factors – this is a recurring theme that when asked about sub cloud factors in particular, where in this case the initial response was negative, upon consideration of the sub cloud factors the responses were more positive. This supports the idea of including consideration of sub cloud factors in this study.

Figure 5-40: Negotiation and Sub Cloud Factors of Compliance



5.7.1.5 Negotiation (specify requirements) with other relationship factors (Compliance) (Spearman correlation)

Table 5-19: Negotiation with other relationship factors (compliance) (Spearman correlation)

Relationship factors	Trust	Ability to negotiate (negotiation)	CSP understands requirements (negotiation)	Risk	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
Effectively specify requirements (negotiation)	moderate 0.516**	NC	NC	Moderate 0.447**	moderate 0.426**	moderate 0.444**	weak 0.266**	Moderate 0.526**

There was a positive and moderate correlation between ability to specify requirements for compliance and all other relationship factors except sufficient information about CSP which had a weak correlation and general ability to negotiate requirements and CSP understands requirements which had no correlation (see Table 5-19). Therefore, there is a link between the perceived ability to negotiate and other relationship factors which means that the ability to negotiate or otherwise has a significant influence on other relationship factors where compliance is concerned.

5.7.1.6 Negotiation (specify requirements) and Security and Privacy

There was a high level of agreement with the idea that the government respondents could specify requirements for security and privacy with 73.8 percent agreeing and 20 percent strongly agreeing with this idea (see Table 5-20).

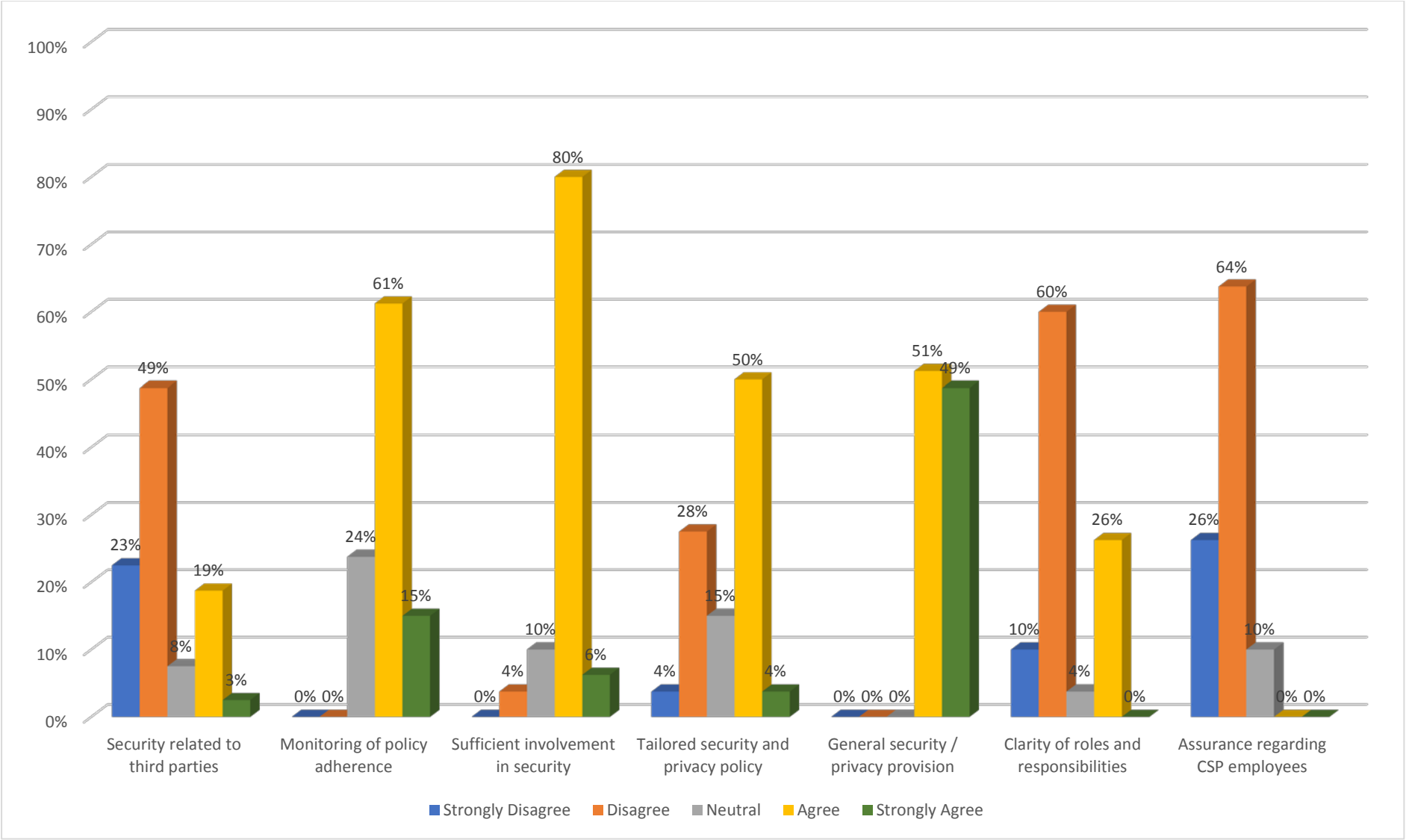
Table 5-20: Negotiation and Security and Privacy Q6C

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0.0	0.0	0.0
	Disagree	0	0.0	0.0	0.0
	Neutral	5	6.3	6.3	6.3
	Agree	59	73.8	73.8	80.0
	Strongly Agree	16	20.0	20.0	100.0
	Total	80	100.0	100.0	

5.7.1.7 Negotiation (specify requirements) and Sub Cloud Factors of Security and Privacy

Respondents gave mixed opinions when questioned about the sub cloud factors of security and privacy. There was very strong agreement with the idea that the government could specify requirements for *General security / privacy provision* with 51 percent agreement and 49 strongly agreeing with this idea, this was followed by *Monitoring of policy adherence* with 61 percent in agreement and 15 percent strongly agreeing, there was also strong agreement, 80 percent, that the respondents could specify requirements for *Sufficient involvement in security* (see Figure 5-42).

Figure 5-41: Negotiation and Sub Cloud Factors of Security and Privacy



As with the other relationship factors and the associated sub cloud factors there was disagreement in the areas that can be considered to be a particular concern to government. *Security related to third parties* received a high level of disagreement at 49 percent disagree and 23 percent strongly disagree, the same was true *Assurance regarding CSP employees* with 64 percent disagreeing and a significant 26 percent strongly disagreeing, and finally, *Tailored security and privacy policy* with 28 percent disagreement and 4 percent strongly disagreeing. Concern about third parties which include those who provide the cloud infrastructure is a concern for government because they need to ensure that they are compliant and protect citizen data.

5.7.1.8 Negotiation (specify requirements) and Performance and Offering

There was also a high level of agreement with the idea that the government respondents could specify requirements for performance and offering, this was evidenced by 60 percent of the respondents agreeing with this idea and 40 percent strongly agreeing, see Table 5-21.

Table 5-21: Negotiation and Performance and Offering Q6D

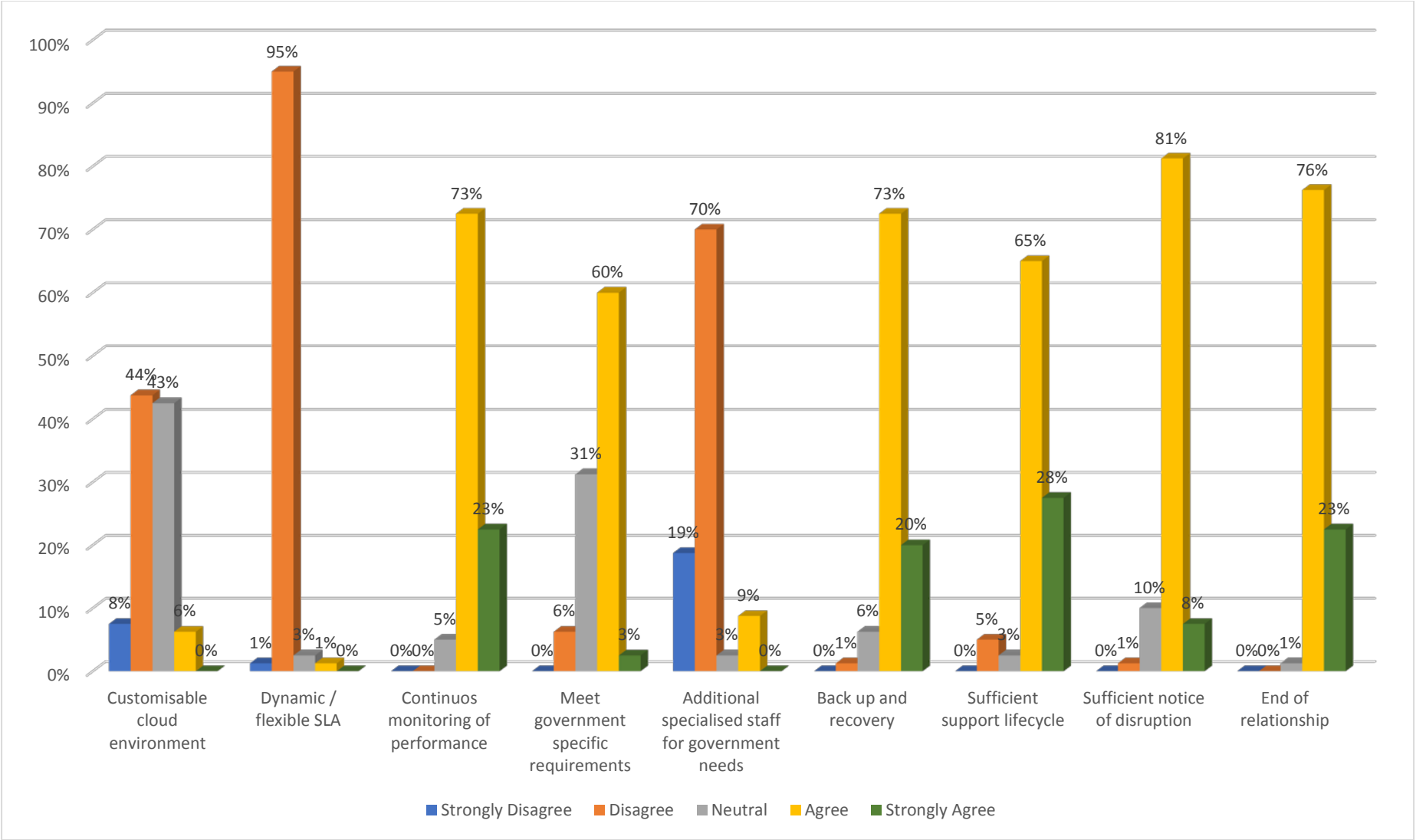
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	0	0.0	0.0	0.0
	Disagree	0	0.0	0.0	0.0
	Neutral	0	0.0	0.0	0.0
	Agree	48	60.0	60.0	60.0
	Strongly Agree	32	40.0	40.0	100.0
	Total	80	100.0	100.0	

5.7.1.9 Negotiation (specify requirements) and Sub Cloud Factors of Performance and Offering

There were also mixed results when the respondents were questioned about the sub cloud factors of performance and offering. Although all the respondents agreed that they could specify requirements for performance and offering, there was disagreement of 70 percent with *Additional specialised staff for government needs* (see Figure 5-43). This shows that government may feel reluctant to adopt the public cloud because they perceive they cannot negotiate specialised staff within the CSP that can be responsible government needs. There was also disagreement that the government could specify requirements for a *Customisable cloud environment* with 44 percent disagreeing, however, it is important to note that 43 percent gave a neutral response. The level of disagreement with the idea that the government

could specify requirements for a *Dynamic / flexible SLA* was very high with 95 percent disagreeing. Thus, there is a lack of confidence that the government can specify requirements for these performance and offering sub cloud factors that are of particular interest and importance to government.

Figure 5-42: Negotiation and Sub Cloud Factors of Performance and Offering



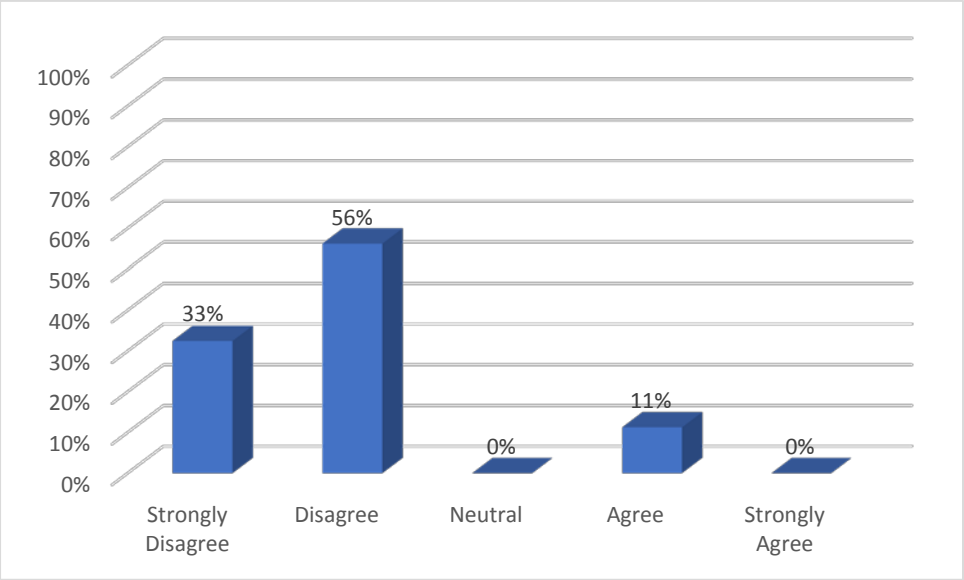
Where there was a very high level of confidence was for *Continuous monitoring and performance* with 73 percent of respondents agreeing and 20 percent strongly agreeing that they could specify requirements for this area. This was followed by *End of relationship* with 76 percent agreeing and 23 percent strongly agreeing, *Sufficient notice of disruption* with 81 percent disagreeing and 8 percent strongly disagreeing and *Sufficient support lifecycle* with 65 percent agreement and 28 percent strong agreement (see Figure 5-43). These are sub cloud factors that although would be important to government, they are part of any standard contract and this is reflected in the high levels of confidence by the government.

5.8 Negotiation (Understand Requirements) Relationship Factor

Part of a successful negotiation is having your requirements understood, in this case government requirements understood by the CSP. The negotiation stage is where requirements are negotiated and if the government feel that the CSP does not understand their requirements then they may feel that they will not achieve what they need from that negotiation. The results show that the vast majority of the government respondents, nearly 90 percent did not feel that the CSP understood their requirements (see Figure 5.44). This result was in sharp contrast to the perception of the ability to negotiate generally. Again, as with the cloud factors and sub cloud factors, here where a specific aspect of a relationship factor is investigated a level of mistrust occurs. Specifically, although there is a high level of trust for negotiation generally, for a specific aspect of negotiation then opinions sharply change.

5.8.1 Negotiation - understand requirements

Figure 5-43: Negotiation – understand requirements



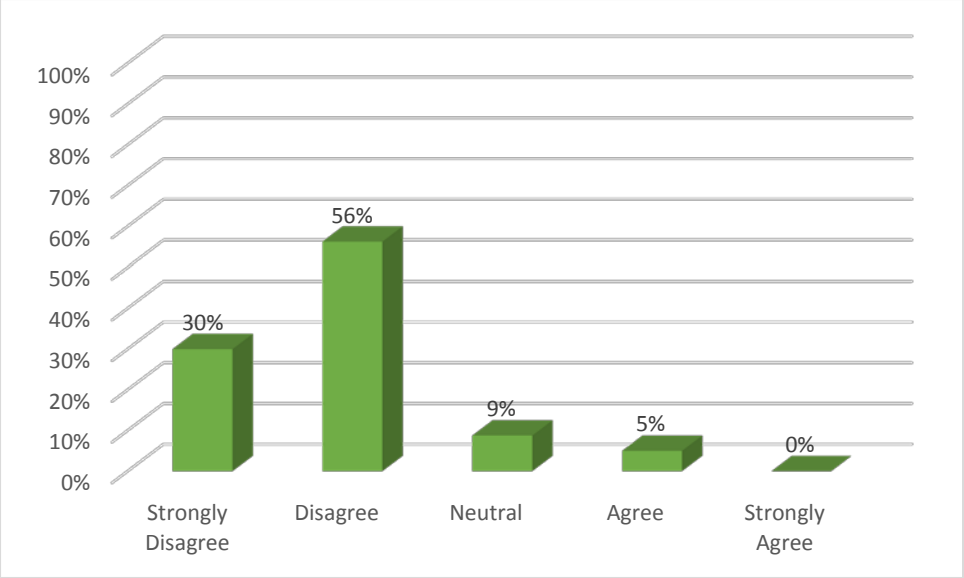
Although there was a high level of confidence by the government that they have the ability to negotiate their requirements, something that they have more control over, within the same negotiation domain they did not feel that the CSP understood their requirements. This was evidenced by 56 percent disagreement and 33 percent disagreement with this idea, and only 11 percent in agreement (see Figure 5.44).

5.8.2 Negotiation – Understand requirements with Cloud Factors and Sub Cloud Factors

5.8.2.1 CSP Understand Governance Requirements

Continuing with the government feeling that the CSP does not understand their requirements, the same was found to be true for governance requirements where 86 percent disagreed and strongly disagreed that the CSP understood governance requirements (see Figure 5.45).

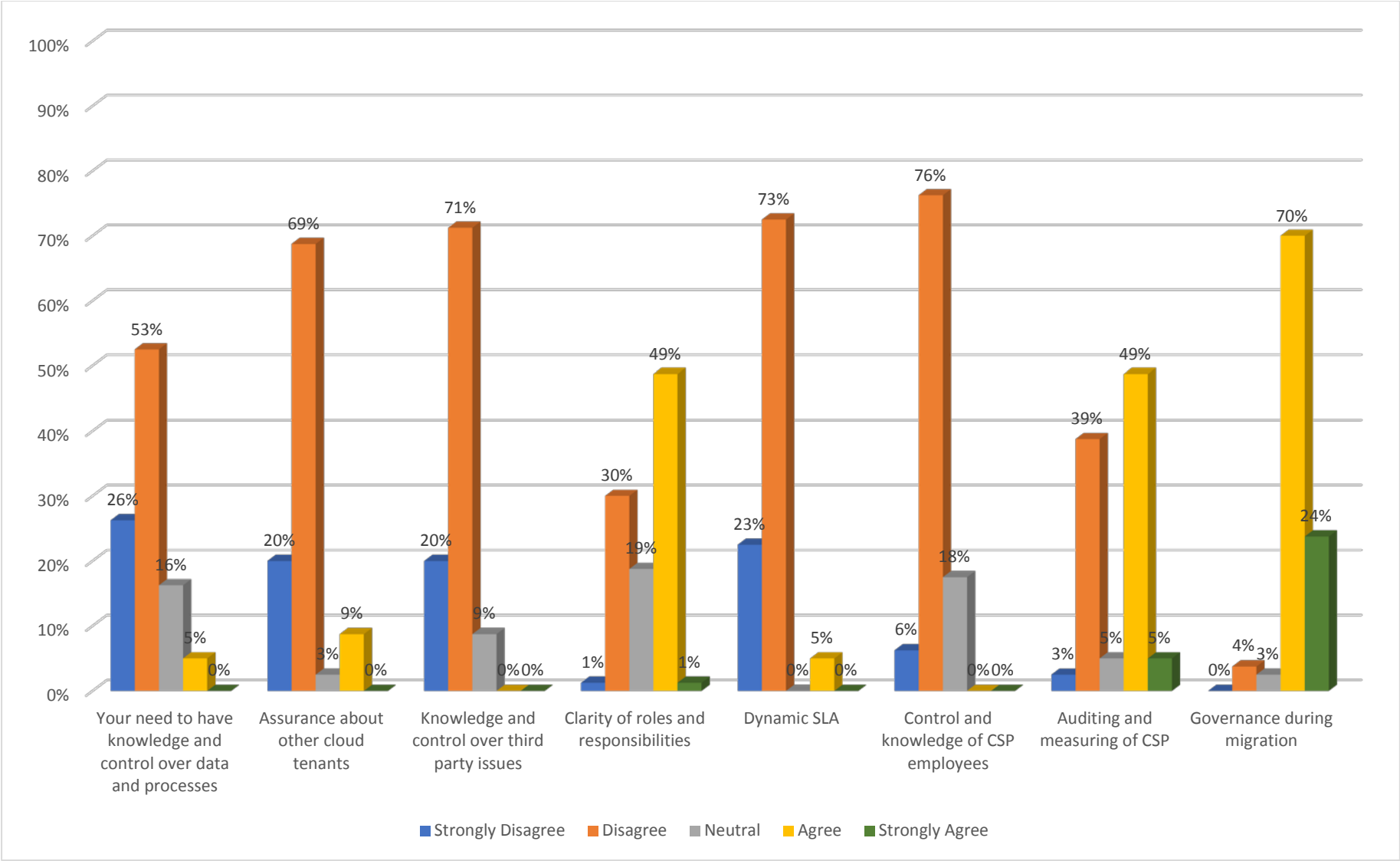
Figure 5-44: Negotiation – understand requirements and governance



5.8.2.2 Negotiation – Understand requirements and Sub Cloud Factors of Governance

The high level of disagreement that government respondents had about having their governance requirements understood was found to be the case for many of the sub cloud factors of governance. There were only three sub cloud factors of governance where they felt that the CSP did understand their governance requirements and this included governance during migration, auditing and measuring of CSP and clarity of roles and responsibilities for governance. Therefore, in these areas the government feel that they are understood, however, in the other areas of governance they feel they are not. For the latter, these are areas of governance that are of particular concern for government. This represents a real concern from the government, that they feel that the CSP does not understand most of their governance requirements, especially governance requirements related to the employees of the CSP, a dynamic SLA with provisions for governance, control and knowledge of third party issues in relation to governance and assurance about cloud tenants. This has serious implications for trust or a perception of risk (see figure 5-46).

Figure 5-45: Negotiation - understand requirements) and Sub Cloud Factors of Governance



5.8.2.3 Negotiation (CSP understands requirements) with other relationship factors (Governance) (Spearman correlation)

Table 5-22: Negotiation with other relationship factors (governance) (Spearman correlation)

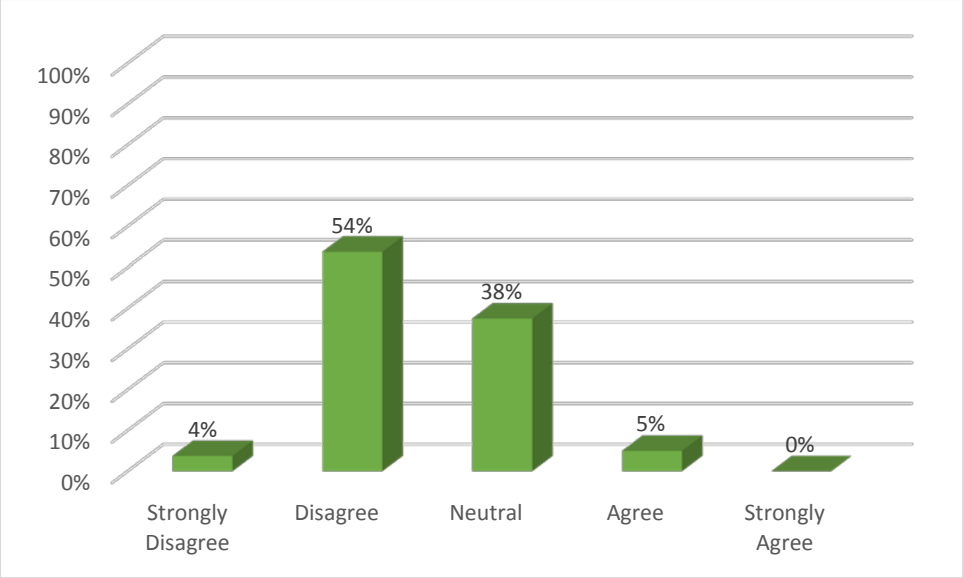
Relationship factors	Trust	Risk	Effectively specify requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
CSP understands requirements (negotiation)	weak 0248*	weak 0.227*	NC	moderate 0.430**	weak 0.338**	moderate 0.446**	weak 0.369**	strong 0.721**

The government's perception that the CSP understands the CSP governance requirements was moderately and weakly associated with other relationship factors for the same cloud factor. It is worth noting that there was a positive strong correlation between CSP understands governance requirements and the perception of a strong reputation of the CSP for governance (see Table 5-22). This means that because there was a negative perception by the government that the CSP understands their governance requirements, there was an associated negative perception of reputation in relation to governance. This has implication for the CSP that they may have a negative reputation for governance because they do not understand governance requirements properly.

5.8.2.4 Negotiation – Understand Requirements and Compliance

The perception by the government respondents that the government understood their requirements was also found to be negative for the cloud factor of compliance with over half of the respondents disagreeing (see Figure 5.47). However, there were a significant number, 38 percent who responded neutral, this means that there is a significant level of uncertainty about the issue of whether respondent felt that the CSP could understand their compliance requirements.

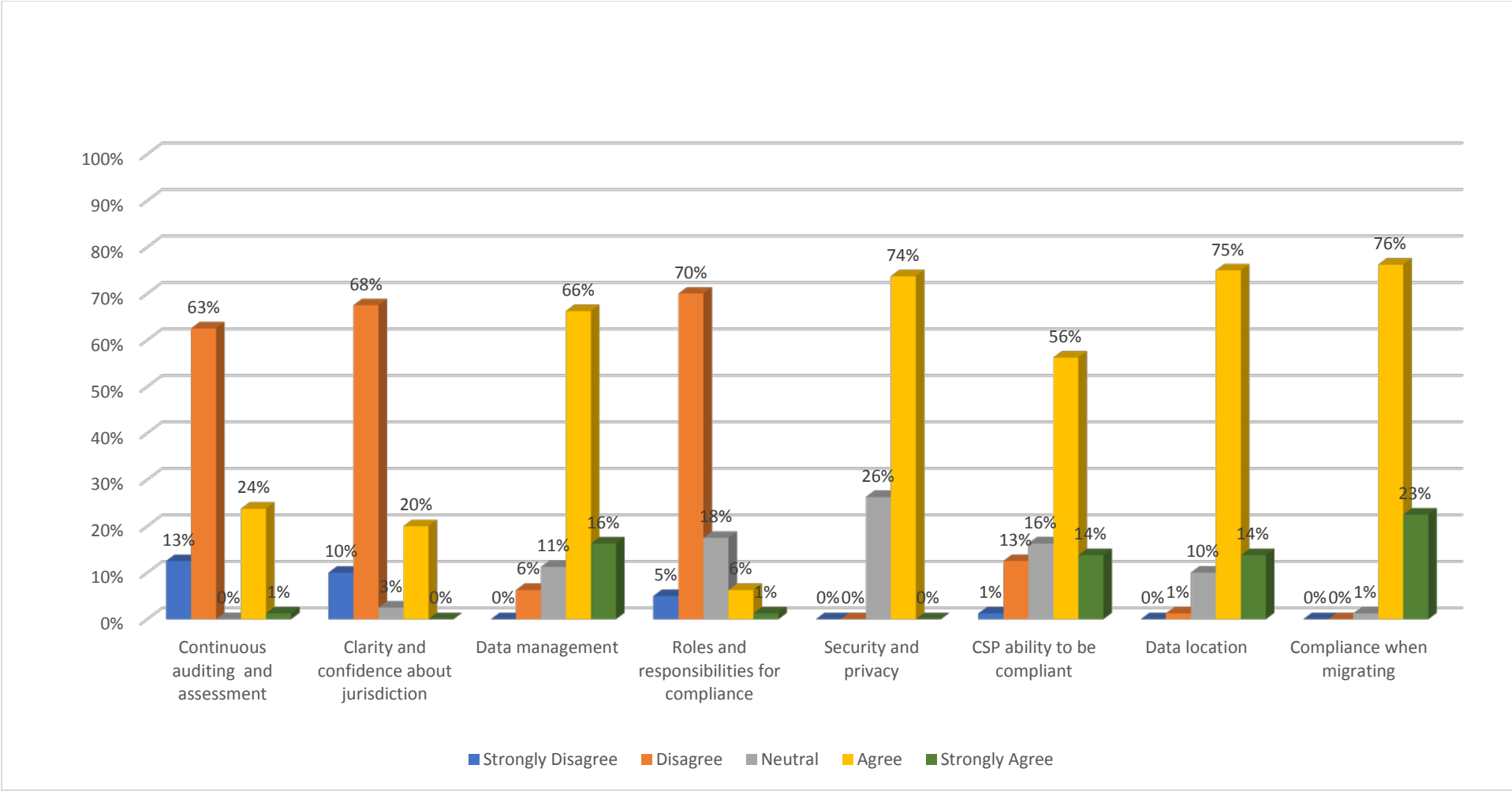
Figure 5-46: Negotiation – Understands requirements Q8B Compliance



5.8.2.5 Negotiation – Understand requirements and Sub Cloud Factors of Compliance

The government felt that the CSP did not understand a number of requirements within compliance, these included *Continuous auditing and assessment*, *Clarity and confidence about jurisdiction* and *Roles and responsibilities for compliance.* However, for the majority of sub cloud factors there was very little concern about having requirements understood (see figure 5-48).

Figure 5-47: Negotiation and Sub Cloud Factors of Compliance



5.8.2.6 Negotiation (CSP understands requirements) with other relationship factors (Compliance) (Spearman correlation)

Table 5-23: Negotiation – Understand requirements with other relationship factors (compliance) (Spearman correlation)

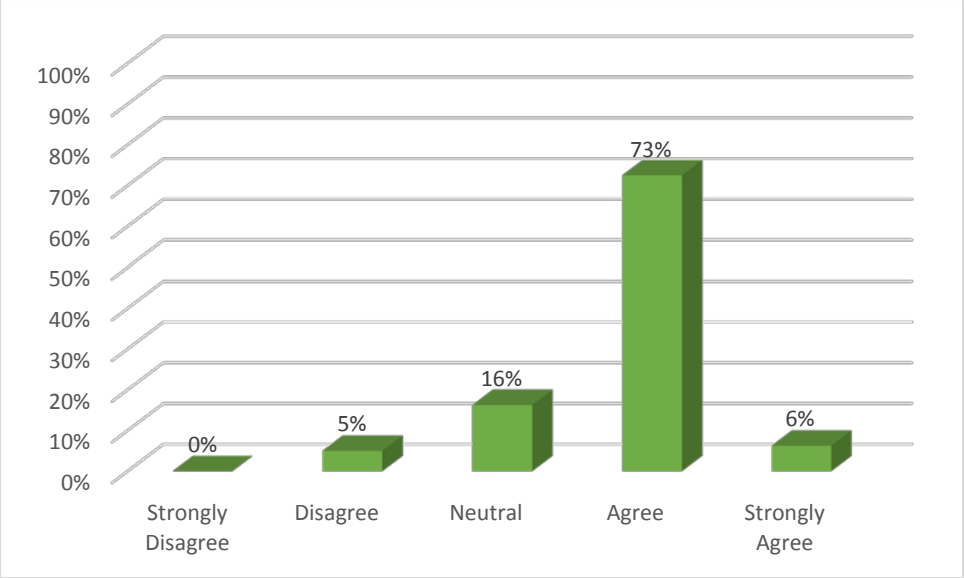
Relationship factors	Trust	Risk	Effectively specify requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
CSP understands requirements (negotiation)	NC	weak 0.249*	Neg weak -0.247*	NC	moderate 0.463**	Neg weak -0.329**	weak 0.374**	NC

There was very little correlation between the government believing that the CSP understands their compliance requirements and other relationship factors. Negative correlations were found between CSP understand requirements and effectively specify requirements and effectively communicate (see Table 5-23). This means that because the government did not feel that the CSP did understand their compliance requirements, there was an associated positive perception that the government could specify compliance requirements and effectively communicate for compliance requirements.

5.8.2.7 Negotiation – Understand Requirements and Security and Privacy

The majority of the respondents, 73 percent agreed and 6 percent strongly agreed with the idea that the CSP understood their security and privacy requirements. Only 5 percent were in disagreement with this idea, but there were 16 percent who responded neutral (see Figure 5.49).

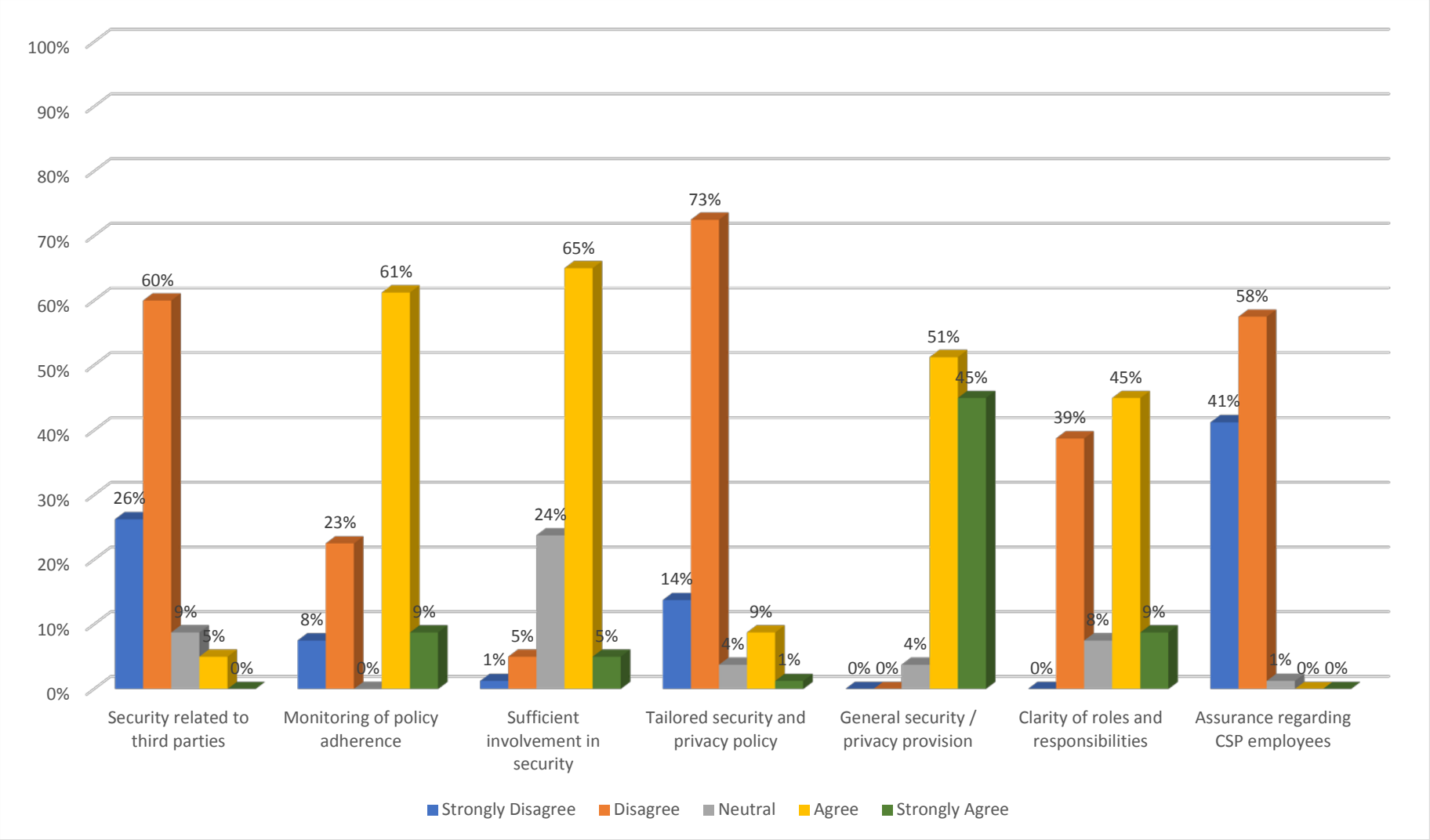
Figure 5-48: Negotiation understand requirements Q8C Security and Privacy



5.8.2.8 Negotiation – Understand requirements and Sub Cloud Factors of Security and Privacy

As for the sub cloud factors of security and privacy there was disagreement with the idea that the CSP understood requirements for sub cloud factors that are a particular concern for government. Specifically, these included *Security related to third parties, Tailored security and privacy policy* and *Assurance regarding CSP employees*. All of these sub cloud factors have been shown to be of a particular concern for government (see figure 5-50).

Figure 5-49: Negotiation – Understand requirements and Sub Cloud Factors of Security and Privacy



5.8.2.9 Negotiation (CSP understands requirements) with other relationship factors (Security and Privacy) (Spearman correlation)

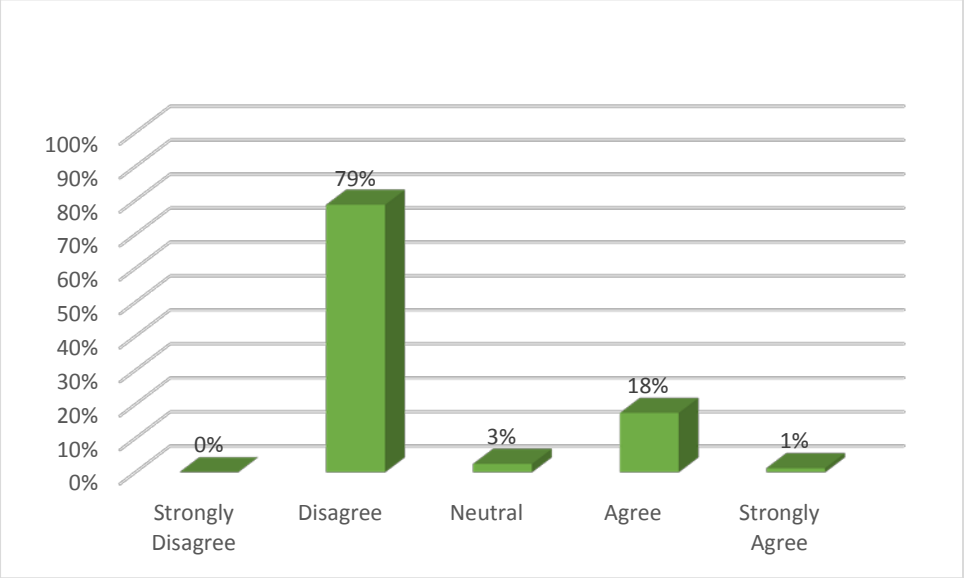
Table 5-24: Negotiation with other relationship factors (security and privacy) (Spearman correlation)

Relationship factors	Trust	Risk	Effectively specify requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
CSP understands requirements (negotiation)	NC	weak 0.309**	moderate 0.437**	weak 0.380**	moderate 0.535**	weak 0.398**	weak 0.397**	weak 0.356**

Between the relationship factor of CSP understands security and privacy requirements and other relationship factors, there were only two correlations that were moderate, these were effectively specify requirements and effectively collaborate (see Table 5-24). Therefore, there was a link between the perceived ability to specify security and privacy requirements and the perception that the CSP understands security and privacy requirements. Because there was a high level of agreement by the government with the idea that the CSP understood their security and privacy requirements, there was an associated positive perception that the government could effectively specify requirements and effectively collaborate.

5.8.2.10 Negotiation – Understanding requirements and Performance and Offering

Figure 5-50: Negotiation Q8D Performance and Offering

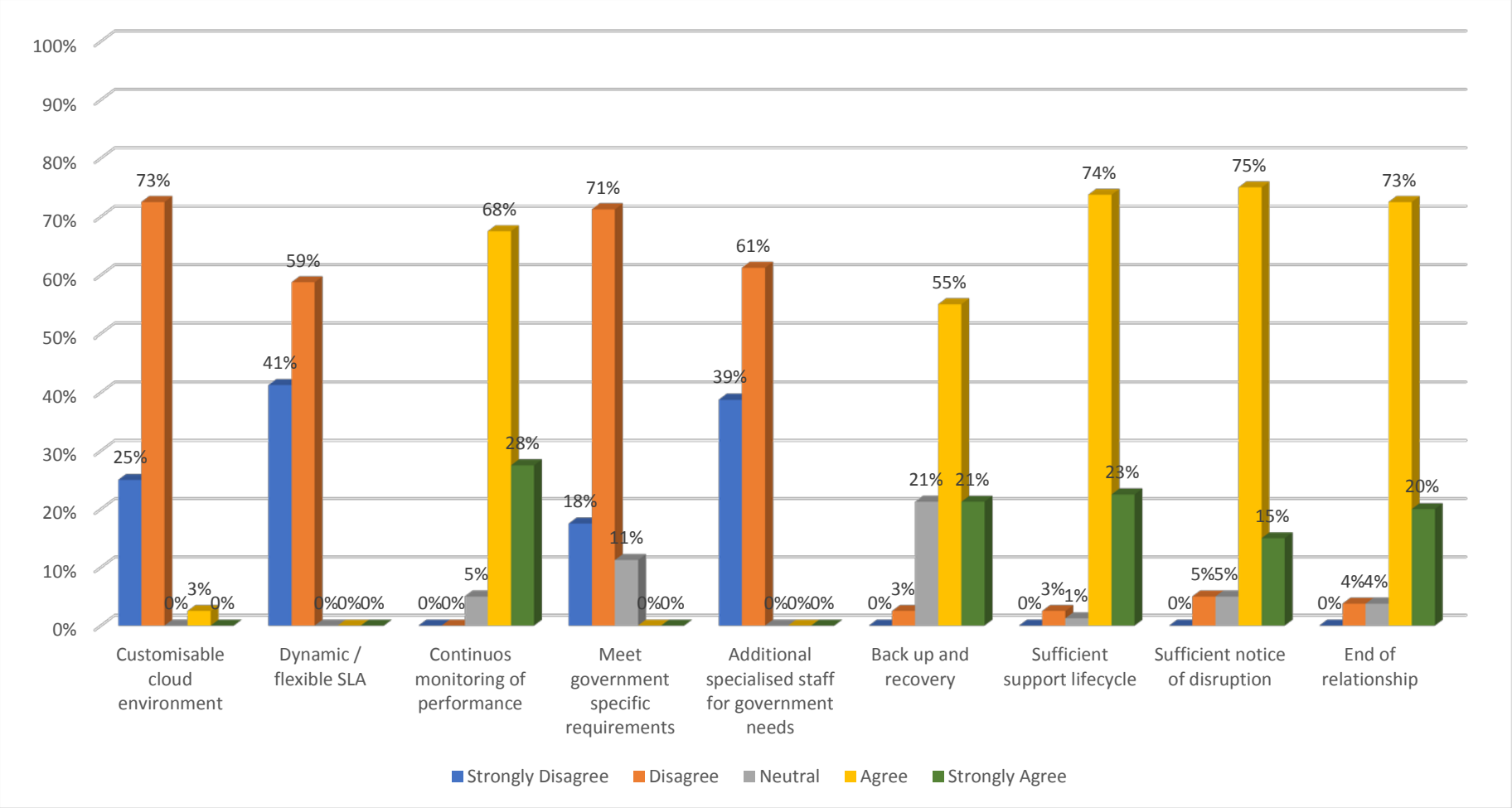


In contrast to security and privacy, where the government were asked about if the CSP understood their performance and offering requirements, they disagreed evidenced by 79 percent disagreement. A significant 18 percent were in agreement (see figure 5-51).

5.8.2.11 Negotiation - Understand requirements and Sub Cloud Factors of Performance and Offering

For the sub cloud factors of performance and offering, there was disagreement with the idea that the CSP understand government performance and offering requirements for those that are a particular concern or relevance to government as suggested by the literature. These sub cloud factors include *Customisable cloud environment, Dynamic SLA, Meet government specific requirements* and *Additional specialized staff for government needs.* Until now this has been a recurring theme where there is a high level of skepticism for these types of sub cloud factors (see figure 5-52).

Figure 5-51: Negotiation Q7 and Sub Cloud Factors of Performance and Offering



5.8.2.12 Negotiation (CSP understands requirements) with other relationship factors (Performance and Offering) (Spearman correlation)

Table 5-25: Negotiation with other relationship factors (performance and offering) (Spearman correlation)

Relationship factors	Trust	Risk	Effectively specify requirements (negotiation)	Ability to negotiate (negotiation)	Effectively collaborate (collaboration)	Effectively communicate (collaboration)	Sufficient information about CSP (reputation)	Perceived positive reputation (reputation)
CSP understands requirements (negotiation)	weak 0.231*	moderate 0.485**	NC	weak 0.247*	NC	NC	NC	NC

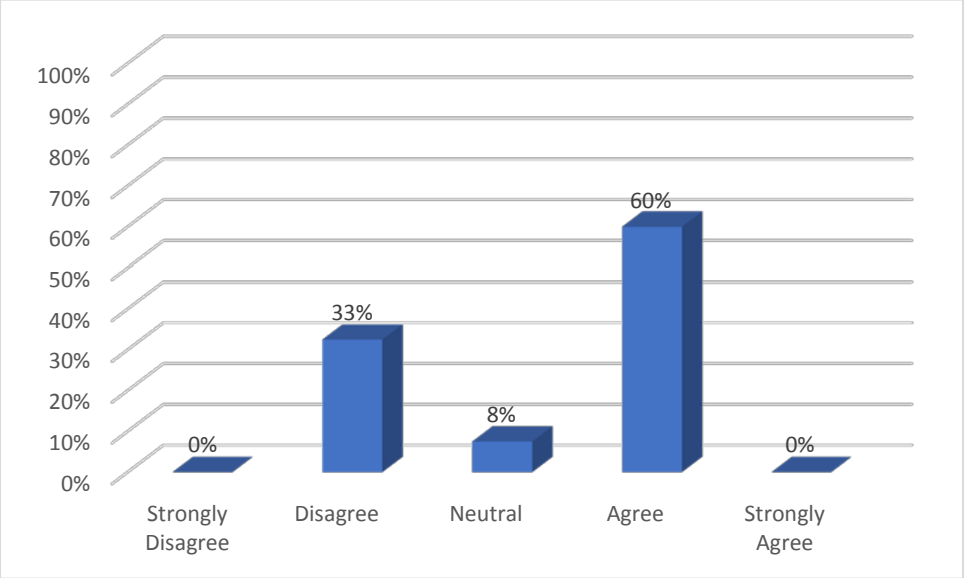
There were no significant correlations between the relationship factor of CSP understands performance and offering requirements and other relationship factors, with the exception of risk with a moderation correlation (see Table 5.25). Therefore, the perception by the government that the CSP understands their performance and offering requirements is not related to other relationship factors.

5.9 Reputation – Relationship Factor

5.9.1 Reputation – general agreement

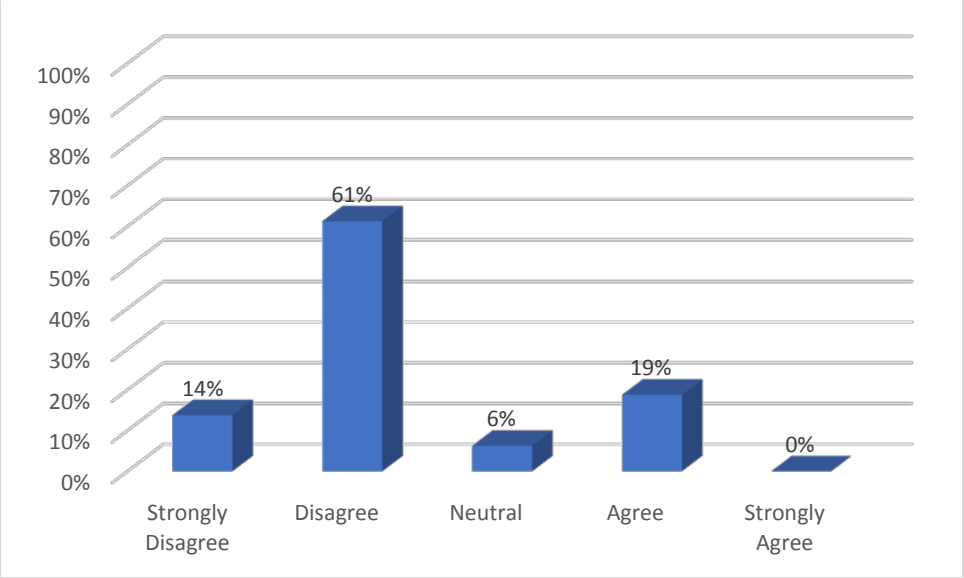
Most of the respondents, 60 percent, agreed with the idea that they perceived a positive reputation of their CSP, however, a significant number of the respondents, 33 percent, disagreed with this idea (see Figure 5-53).

Figure 5-52: Reputation General



Despite the fact that there was generally a level of agreement with the idea that the government agree that they perceive a positive reputation, there was a high level of disagreement with the idea that the government have sufficient information about the CSP. This was evidenced by the fact that 61 percent disagreed and 14 percent strongly disagreed with this idea, however, a significant 19 percent were in agreement (see Figure 5.54). Therefore, this means that having sufficient information is not linked to the perception of a positive reputation.

Figure 5-53: Reputation – Sufficient Information



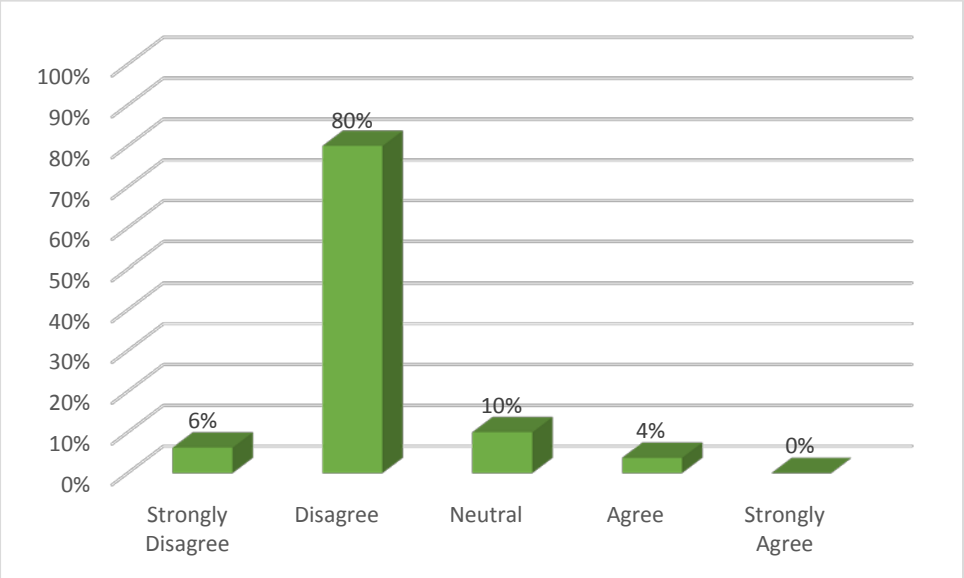
5.9.2 Reputation with Cloud Factors and Sub Cloud Factors

Reputation was analysed against the cloud factors and sub cloud factors in order to determine how the government felt about the reputation, as a relationship factor, of the CSP in relation to the cloud.

5.9.2.1 Governance

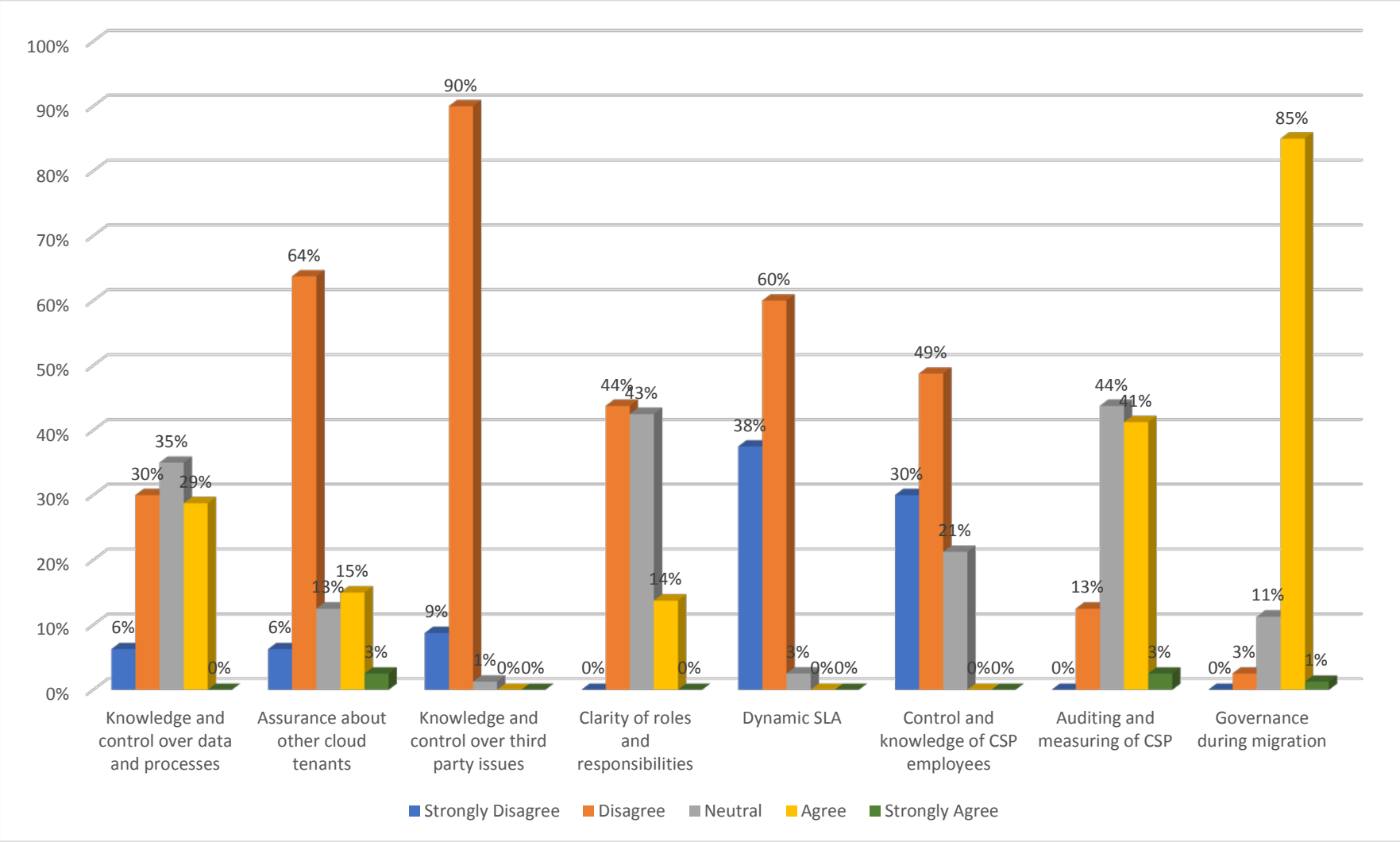
Where the government respondents were asked about whether they perceived a positive reputation for governance the vast majority, 80 percent, disagreed (see Figure 5-55).

Figure 5-54: Reputation and Governance



5.9.2.2 Reputation and Sub Cloud Factors of Governance

Figure 5-55: Reputation and Sub Cloud Factors of Governance

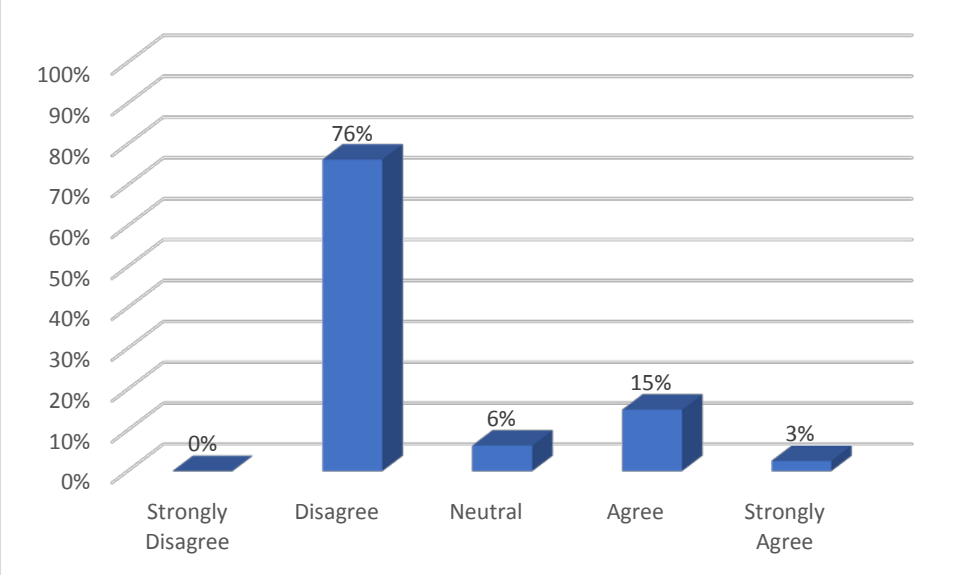


The high level of disagreement with the idea that a positive reputation is perceived in relation to governance was further confirmed by the fact that the respondents disagreed they perceived a positive reputation for most of the sub cloud factors of governance. Specifically, there was a high level of disagreement with *Knowledge and control over third party issues* at 90 percent, *Assurance about other cloud tenants* at 64 percent disagreement, *Dynamic SLA* at 60 percent disagreeing and 38 percent strongly disagreeing and *Control and knowledge of CSP employees* 49 percent disagreeing and 30 percent strongly disagreeing (see Figure 5-56).

There were only two sub cloud factors where the respondents agreed with the idea that they perceived a positive reputation, these were *Governance during migration* with 85 percent agreeing and *Auditing and measuring of CSP* with 41 percent agreeing, however, for this sub cloud factor there were more respondents at 44 percent that gave neutral as their answer (see Figure 5-56).

5.9.2.3 Reputation and Compliance

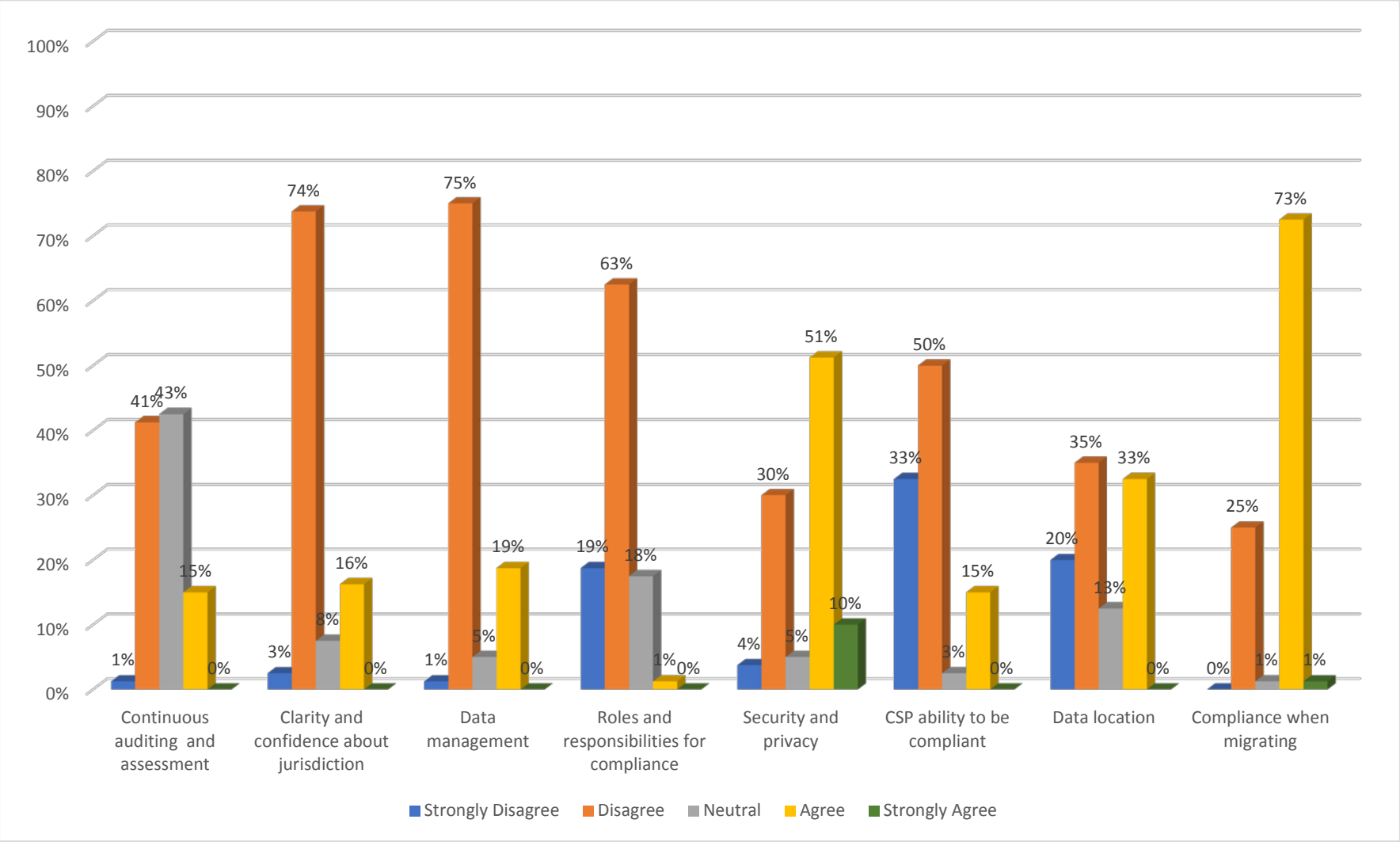
Figure 5-56: You Perceive a Positive Reputation in Relation to Compliance



The respondents clearly did not perceive a positive reputation in relation to compliance where 76 percent disagreed with this idea and only 18 percent agreed (see Figure 5-57).

5.9.2.4 *Reputation and Sub Cloud Factors of Compliance*

Figure 5-57: Reputation and Sub Cloud Factors of Compliance

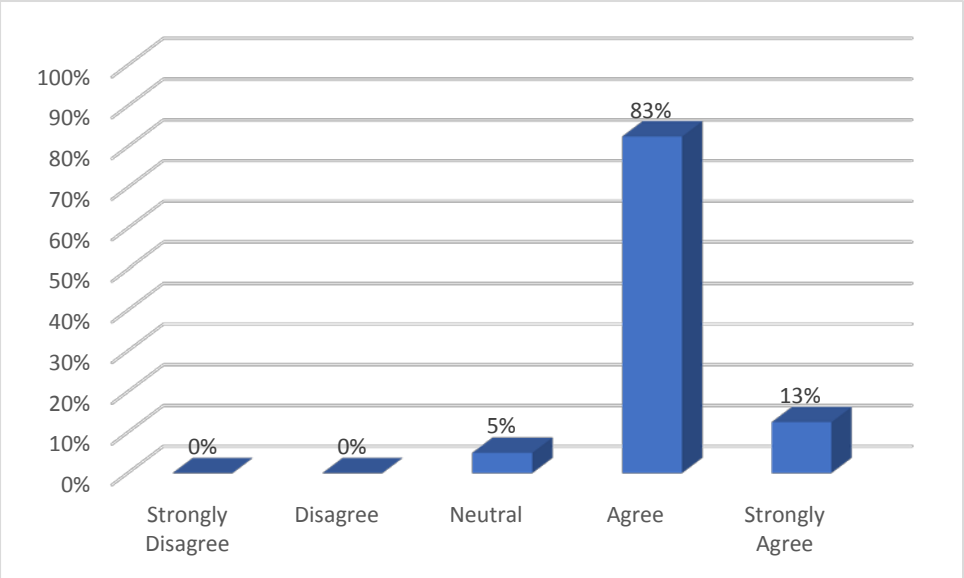


When the respondents were questioned about the sub cloud factors of compliance, the results confirmed the idea that the respondents did not agree that they perceived a positive reputation in this area. Particularly, there was a high level of disagreement for *Data management* at 75 percent and *Clarity and confidence about jurisdiction* at 74 percent and *Roles and responsibilities for compliance* 63 percent disagreement and 19 percent strongly disagreeing. There was a high level of disagreement for *CSP ability to be compliant* at 83 percent overall. The only sub cloud factor for compliance where a positive reputation was perceived was for *Compliance when migrating* with 73 percent agreeing (see Figure 5-58).

5.9.2.5 Reputation and Security and Privacy

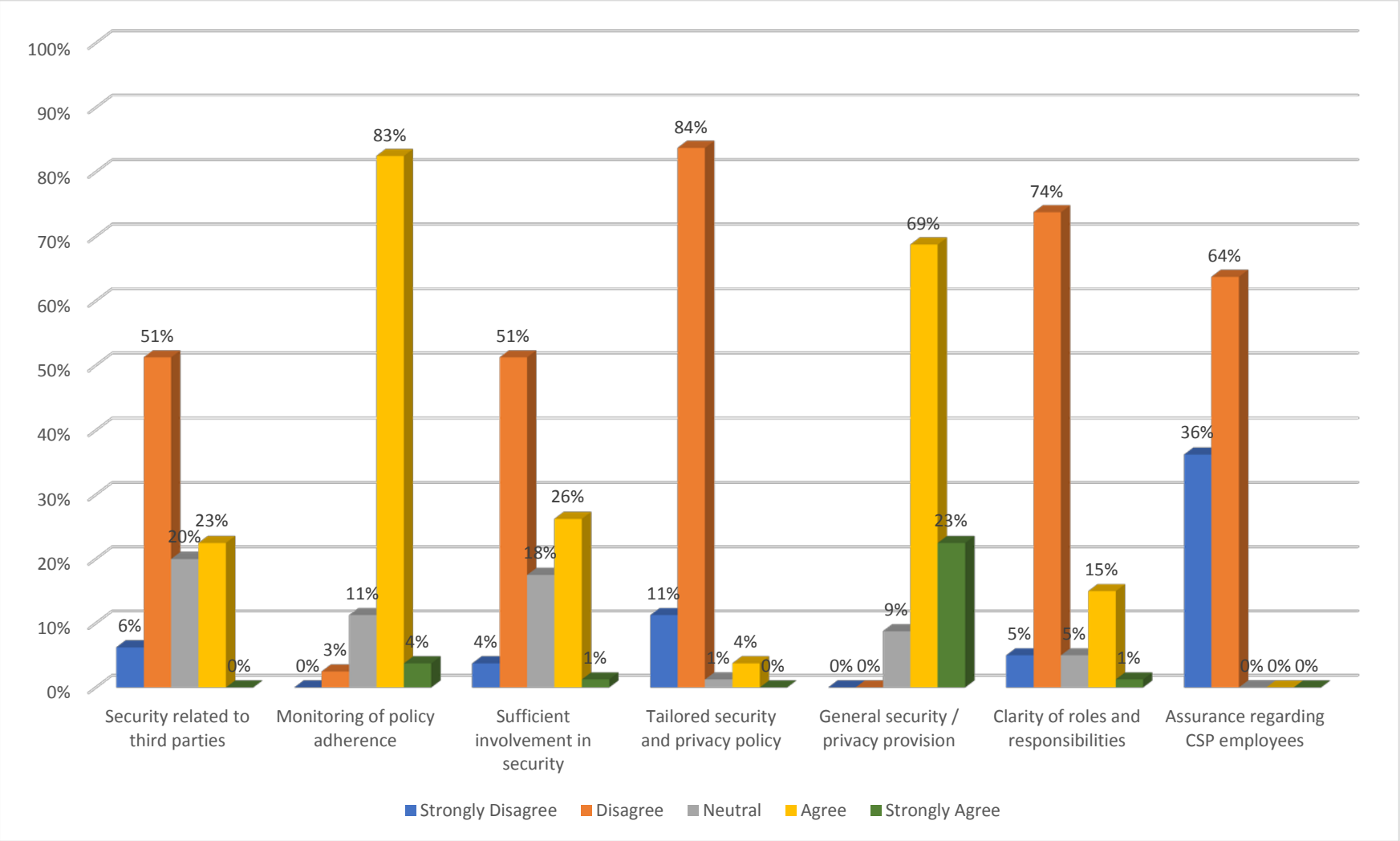
In the above it was shown that the respondents perceived a poor reputation for compliance, however, where the respondents were questioned about security and privacy there was a high level of agreement that they perceived a positive reputation, this was evidenced by the fact that 83 percent agreed and 13 percent strongly agreed with this idea with none of the respondents disagreeing. Therefore, the government respondents do not see a problem with security and privacy generally because they perceive a positive reputation (see Figure 5-59).

Figure 5-58: You Perceive a Positive Reputation in Relation to Security and Privacy



5.9.2.6 Reputation and Sub Cloud Factors of Security and Privacy

Figure 5-59: Reputation and Sub Cloud Factors of Security and Privacy



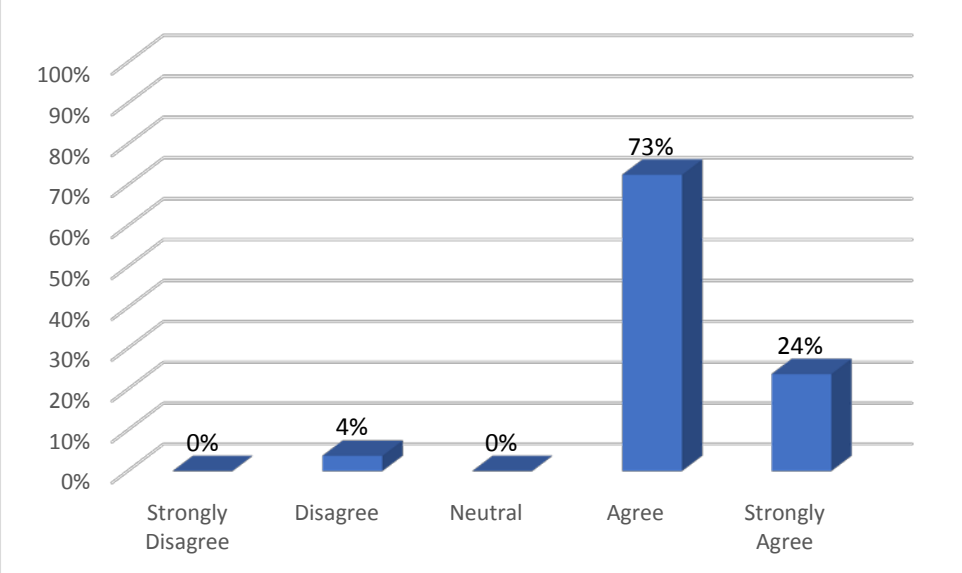
Where the respondents were asked about the perceived reputation for the sub cloud factors of security and privacy then the high level of a positive reputation is not seen for most of the sub cloud factors. There was a particular high level of disagreement with the idea of a positive reputation for *Assurance regarding CSP employees* where 64 percent disagreed and 36 percent strongly disagreed, there was also a high level of disagreement for *Tailored security and privacy policy* at 84 percent and *Clarity of roles and responsibilities* with 74 percent disagreement (see Figure 5-60).

There were only two sub cloud factors for security and privacy where a positive reputation was perceived and they were *Monitoring of policy adherence* with 83 percent agreement and *General security / privacy* with 69 percent agreeing and 23 percent strongly agreeing (see Figure 5-60). In reference to latter sub cloud factor it is a factor that is closely related to security and privacy as a cloud factor and for both there was a positive reputation. It is clear from these results that although there may be a positive reputation for security and privacy, where respondents are asked about the particular aspects of security and privacy then they start to say that they do not perceive positive reputations.

5.9.2.7 Reputation and Performance and Offering

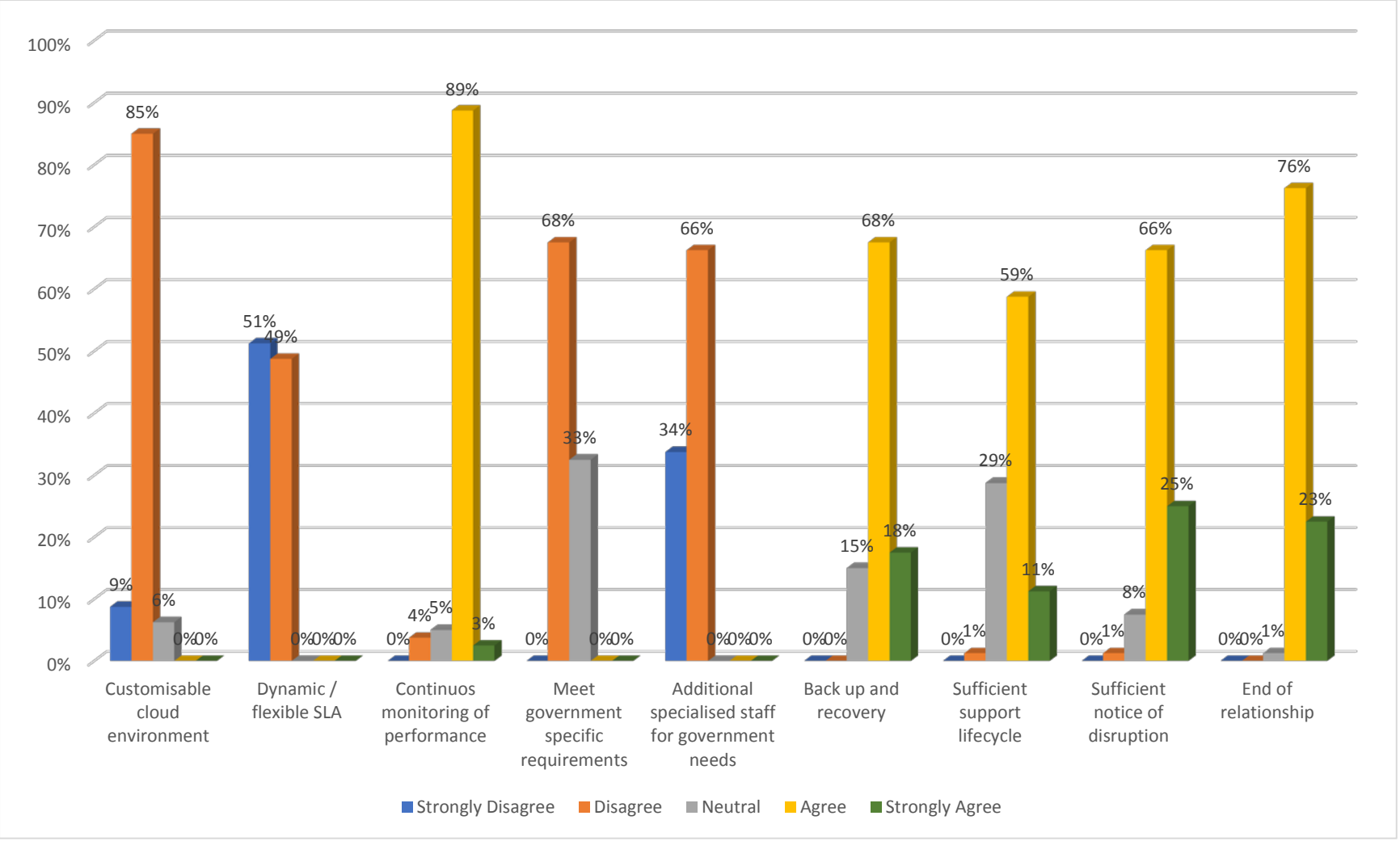
There was also a very high perception of a positive reputation for performance with 73 percent agreeing and 24 percent strongly agreeing and only 4 percent disagreeing (see Figure 5-61).

Figure 5-60: You Perceive a Positive Reputation in Relation to Performance and Offering Q18D



5.9.2.8 Reputation and Sub Cloud Factors of Performance and Offering

Figure 5-61: Reputation and Sub Cloud Factors of Performance and Offering



There was also a positive perception of reputation for most of the sub cloud factors of performance and offering. Where there was a level of disagreement with this idea was again in relation to those sub cloud factors of performance and offering that are of particular concern or relevance to government. Specifically, these included *Dynamic / flexible SLA* with 49 percent disagreeing and an even greater 51 percent for strongly disagreeing. This was followed by *Customisable cloud environment* with 85 percent in disagreement and *Meet government specific requirements* with 68 disagreeing and *Additional specialised staff for government needs* with 66 percent disagreeing and 34 percent strongly disagreeing (see Figure 5-62).

5.10 Conclusion

The findings showed that there was trust generally in the CSP but where respondents were asked about trust for specific cloud issues sometimes there was a negative response. This was found to be the case for governance and compliance. However, for security and privacy and performance and offering there was a positive perception of trust. Moreover, where the sub cloud factors for all cloud factors were considered, there was also a wide variation in trust, where there was strong trust for some sub cloud factors and a significant lack of trust for others, and rarely were there mixed opinions for sub cloud factors. The variation in these perceptions of trust coincides with sub cloud factors that are either a specific concern or relevance for government or sub cloud factors that are standard in SLAs where there is much less concern. For example, there was a low perception of trust for other cloud tenants, third parties, CSP employees and a dynamic SLA, all of which are especially important for government in the cloud, but for general areas such as governance during migration there was a high perception of trust. This pattern was found to be true for most of the sub cloud factors of governance, compliance, security and privacy and performance and offering where a high level of certainty was shown.

These ideas were also found to be true for all of the relationship factors, where there was more negativity in those cloud areas that are especially important for government. This shows that there is certainty in the opinions of the respondents because of the variation in responses.

In reference to analysis between relationship factors for each of the cloud factors, generally there was little correlation. Where correlations were revealed, these are relevant to the study because they offer a better understanding the relationship. For example, a correlation between

trust in governance and an ability to negotiate for governance contributes to recommendations for the CSP because it informs them that in order to, for example, improve negotiation there needs to be a certain level of trust. These correlations between the various relationship factors considered against the cloud factors offered a deep insight into the relationship and how relationship factors affect each other in consideration of the different cloud factors.

Despite there being mostly weak and moderate correlations, the results did reveal some strong correlations that can inform the CSP about the changes they can make. For example, a strong correlation between trust in compliance and the ability to effectively collaborate for compliance would inform the CSP that they could improve collaboration to increase trust in the public cloud, or vice versa.

Overall, these findings give a detailed picture of the relationship issues and associated cloud issues towards understanding the overall reluctance of government to migrate to the public cloud.

6 Results and Analysis - Interviews

Objectives

- **Present the findings of the interviews**
- **Present the analysis of interviews**
- **Present derived themes**

6.1 Introduction

The results of the interview are presented in this chapter. The first section deals with an overview about how the participants to the interview feel about the relationship factors, namely; trust, risk, negotiation, collaboration and reputation and the cloud factors, namely; governance, compliance, security and privacy and performance and offering.

The second section offers a more in-depth insight into the relationship reasons and associated cloud factors towards understand why the Saudi government is reluctant to place sensitive data and critical systems in the public cloud.

Table 6-1: Participant Information

Participant	Organisation	Position	Ministry	Participant code
Participant 1	National Information Centre	Director – department of distributed systems	Ministry of Interior	P1NIC
Participant 2	National Information Centre	Cloud consultant	Ministry of Interior	P2NIC
Participant 3	National Information Centre	Cloud specialist	Ministry of Interior	P3NIC
Participant 4	Saudi Customs	IT specialist	Ministry of Finance	P4CUST
Participant 5	Saudi Customs	IT specialist	Ministry of Finance	P5CUST
Participant 6	Saudi Customs	IT specialist	Ministry of Finance	P6CUST
Participant 7	Immigration	IT specialist	Ministry of Interior	P7IMM

Participant 8	Immigration	IT specialist	Ministry of Interior	P8IMM
Participant 9	Immigration	IT specialist	Ministry of Interior	P9IMM
Participant 10	Ministry of Finance	IT procurement	Ministry of Finance	P10MOF
Participant 11	Ministry of Finance	IT procurement	Ministry of Finance	P11MOF
Participant 12	Ministry of Finance	IT specialist	Ministry of Finance	P12MOF

The Ministry of Finance Saudi Arabia, Saudi Customs which is under the Ministry of Finance, the Saudi Immigration Department and the National Information Centre, both under the Ministry of Interior are the organisations that the respondents were sampled from.

6.2 Current Situation

There was indication from some of the participants that they were at the consideration stage of the cloud which included testing, however, they had not started using the cloud for government purposes.

One of the participants said the following:

> *We have had testing with some cloud providers* (P7IMM)

The idea that there is not a direct working relationship and that they are still at the consideration for the public cloud is found in the following statement in response to a question about the relationship with the service provider:

> *In this term there are no direct relation, the only relationship channels is during the workshop and seminar* (P4CUST)

However, the National Information Centre, which overall is responsible for government IT and IS policy in the country, had more to say about the current relation with CSPs. One of the respondents said the following:

> *We understand the importance of the public cloud and it is something that is part of our cloud strategy. Until now we have worked with CSPs in this area and have tested the public cloud* (P3NIC)

The researcher probed further and asked if that was with sensitive data, the respondent said the following:

> *No, we do not test with sensitive data* (P3NIC)

6.3 Concerns about security and privacy

Concern about security and privacy was a recurring theme throughout the interviews from all of the participants. When one of the participants was asked about the concerns that they have about the public cloud, they said the following:

> *Confidentiality and security of government data. The cloud in this area is still not mature enough* (P7IMM)

There was a significant amount of mention that because it was the government data there was concern that there would be a breach of privacy in terms of protection of the data rights of the citizens, this is clearly expressed in the following statement:

> *Since this is a Government Organization so, there is no guarantee it would not violate those rights Protection of data rights* (P4CUST)

One of the fears is that the cloud services in Saudi Arabia are in the hands of the largest local telecommunications company which is often a target for hackers. This concern is not associated with any relationship factors and is simply a perception of a security threat in the cloud. The following statement illustrates this idea:

> *and if you mean security trust I can said we have some fears since currently who is leading the cloud service on this country is the biggest telecommunication companies which are they been target and frequently attacked from the hackers* (P7IMM)

In the statement in the above the respondent says that although there is trust in security, there are concerns about the local CSP who are telecommunication companies that are frequently attacked by hackers.

The perception of risk was also associated not only with external threat to security but also internal threats of the CSP themselves, in response to the question about whether the participant perceived any risks in relation to their CSP, they said the following:

> *Yes, because of lack of the right resources* (P7IMM)

Within the social context of the cloud service relationship there are many different actors which include the cloud service provider (CSP), the cloud provider (CP), other users and certification bodies. Not only did the participants see the threat to security coming from external threats in the form of attacks, or from a weakness of the CSPs themselves, but they also perceived a security threat from other users of the cloud and even cited the issues of multi-tenancy:

> *Shared infrastructure (i.e. Multi-Tenancy) raises a huge security concerns* (P8IMM)

A perception of risk has been acknowledged in relation to the sensitive data of government and given as a reason for not currently adopting the cloud. In response to the question about whether there are plans to adopt the public cloud one of the participants said the following:

> *There is a plan but because the data is very sensitive, this plan is postpone* (P4CUST)

In fact, there was acknowledgement that the public cloud is not suitable for sensitive data, one of the participants said the following:

> *Currently we have private cloud for sensitive data, and uses public cloud for non-sensitive transactions* (P4CUST)

Evidence of a perception of risk is also found in the fact that there has been a reluctance to completely adopt the public cloud; one of the participants said the following when asked if they perceived any risks with their service provider:

> *Not for our situation as we limit the public cloud use* (P8IMM)

6.4 Trust

There were mixed views about the issue of trusting the CSP. One of the themes that emerged from the interviews was that many of the participants expressed ideas that were related to what they felt were the qualities of trust.

One of the participants included both morality and professional conduct as attributes of trust, they said the following statement:

> *am not sure, but this is depend and demonstrate a commitment to a moral standard of professional behavior, which they uphold at all times* (P4CUST)

In the statement in the above where the respondent was asked about trust they were not sure, but they did say that trust would depend on whether or there was moral and professional conduct on behave of the CSP.

The qualities of trust were also expressed as an idea about reciprocation, one of the participants said the following:

> *We can trust the cloud provider, we give them our data and trust them but they have to return the trust because it works both ways* (P8IMM)

The idea of trust was also associated with the idea of careful selection. Where there is control over the decision-making process and where a user has more information about the CSP, there will be less uncertainty and therefore, more trust. This idea is clearly emphasised in the following statement:

> *We do trust our suppliers, and carefully select our public cloud provider* (P8IMM)

There were some generally positive responses about trust, the following responses indicate that generally there is trust, however, there is some indication of caution where specific issues are concerned. One of the respondents said the following;

> *Yes, I trust the service provider I don't have any problems as long as they know how important security is for us, then I don't have any issues* (P3NIC)

Another respondent also expressed general trust, but in consideration of more specific issues:

Yes, I do we have had a relationship for a while now so we know them very well so that is why I trust them. However, I do worry sometimes about complying with the law, sometimes I worry that I can trust them about this (P2NIC)

Overall, although there was trust it often came with conditions, or there was more certainty about trust where specific issues were concerned. In the statement above there was specific concern about trusting the CSP complying with the law.

6.5 Negotiation

There was the idea that negotiation with the service provider would be difficult because it is about a government and highly sensitive data and that negotiation about the cloud could breach national security, the following statements clearly highlight this issue:

Currently I do not think so because still we have sensitive data due to National Security, which should be maintain and protected (P4CUST)

And

We can negotiate effectively but only if they understand that we have some very special requirements to protect our data, especially about the citizen (P9IMM)

More generally, negative sentiments were expressed about negation with the CSP, where one participant said in response to whether or not they could negotiate with their CSP:

Unfortunately, no. I don't feel that they are easy to negotiate with (P8IMM)

Another respondent said something similar but also mentioned the idea of a standardised where they mentioned the idea of a fixed service offered by CSPs:

I don't think that we really have the opportunity to negotiate with the CSP because they offer a fixed service (P10MOF)

In relation to negotiation and government requirements, one of the participants said the following:

I think they will be difficult to negotiate because they do not understand what we need as a government, they are not used to working with us only with companies (P11MOF)

In the statement above the respondent was saying that the government feel that they find it difficult to negotiate because the CSP do not have experience of government, and only have experience with private companies.

However, not all of the responses were negative in this regard:

> *I think we have a positive relationship with the provider and we have negotiated before for security provision, as long as they understand us I think we can negotiate all of our cloud needs* (P6CUST)

Overall, where there were negative ideas about the ability to negotiate is was often related to the concern that the CSP will not understand government needs, especially those related to security and privacy of government data.

6.6 Collaboration

One of the key features of the cloud is that it is not simply a product that an organisation buys but rather is an ongoing service with an ongoing relationship that requires collaboration in order to be effective. There was some negative opinion about collaboration from the respondents. One of the respondents indicated that they only receive the service without any collaboration:

> *There is no cooperation. Just to get service* (P10MOF)

Another respondent indicated that the channels for collaboration were not properly established:

> *We could collaborate, I don't have any problem with that, but the problem is it is not clear who we should be working with, we should know who we can speak to in the cloud provider* (P2NIC)

There were indications that generally there was a perception that government could effectively collaborate with the CSP, this was evident in the following statements:

> *In our department we have worked with more than one cloud provider, and generally we can collaborate effectively I don't see any problems* (P6CUST)

One of the respondents highlighted the importance of effective collaboration:

Yes we have to collaborate with the provider and keep a continuous relationship with them (P5CUST)

The researcher then probed further into this idea and asked why it was important to collaborate, the participant responded the following:

They have to understand our needs and we have to make sure that they do what we want because they don't fully understand our needs as a government department (P12MOF)

The idea of specific needs of government was a recurring idea where respondents were questioned about collaboration. One of the respondents felt that collaboration with the CSP was important because of security and privacy reasons:

We keep a lot of sensitive data especially about the citizen and the service provider needs to work closely with us to make sure that the data is protected (P1NIC)

Another respondent echoed a similar idea:

Yes we need to know how they will manage our data because we are responsible for that data (P7IMM)

Here it can be seen that there was a need to collaborate with the service provider in order to protect citizen data and to make sure that it is managed properly. Overall, although there is generally a positive attitude towards collaborating with the CSP, the only real concerns in this area were related to the protection of sensitive data.

This emerging idea that there was a link between collaboration and concern of the data was further supported by two respondents that acknowledged the idea that in order to achieve governance over data collaboration is required, however, it is not always the case that collaboration is effective and leads to the required level of governance:

We need to be able to know where our data is all of the time and we should be able to manage the data anytime we want, so yes we need to collaborate with the service provide and have a positive relationship with them, but I don't think we can collaborate to achieve this that we can manage and control our own data (P1NIC)

In the statement above there is acknowledgement that there is a need to collaborate with the CSP, however, there is doubt that management and control of data can be collaborated for.

Similarly, another respondent said the following:

> *A good collaboration with the provider is very important because we need to work with the provider so we have a level of oversight over the data that we put in the public cloud but even if we have a good relationship with them we can never really control our data, you have to accept that you will lose some control when you use the public cloud* (P3NIC)

Being kept informed by the service provider was an area that was questioned and it was closely associated with collaboration by the researcher. As part of the collaboration it is important that the CSP keeps the customer informed about the status of their data. In response to the question about whether or not participants felt they were informed the following response was received:

> *It would be a very strict requirement that we are kept informed about our data, as you know we are not comfortable with our data being held outside of the country so you can understand why we need to know where the data is* (P1NIC)

6.7 Emerged Themes

In addition to the ideas that were revealed about the considered relationship factors of this study, there were a number of different themes that emerged from the analysis of the interview data. These themes give further insight into the opinions about the public cloud and possible reasons for lack of adoption.

6.7.1 Lack of understanding of the public cloud

Some of the participants gave responses that showed that they did not fully understand the concept of the public cloud. In response to the question about whether they currently have plans to adopt the public cloud one of them said the following:

> *Depends where is data hosting, for government they prefer to host their data in any government premises for commercial they prefer to host data inside country* (P11MOF)

From the statement above it is clear that government prefer to host their data in their own premises, but if they do use a cloud from a private company then the data should stay within the country.

Further evidence that there was a misunderstanding about the nature of the public cloud was expressed in the following statement:

> *but we can benefit from the benefits that the public cloud gives and implement the models of the public cloud at the centre, for example like Amazon is providing the service of the cloud and also other companies. Maybe we can build our own model of public cloud that we host at the centre and provide it to parts of interior ministry and the government can take benefits from it* (P2NIC)

In the statement above the participant says that the public cloud or the public cloud model can be adopted by the government organisation, that this government organisation can build their own cloud based on ideas from, for example, the Amazon public cloud, and be hosted at the NIC for other parts of the Ministry for Interior to use, however, by definition this is not a public cloud it is a private cloud. Therefore, there is a clear lack of understanding of the nature of the public cloud in this case.

Further misunderstanding not only of the nature of the public cloud but also its benefits are expressed in a further statement by the same respondent. When asked if he means to take control of the public cloud under the administration of his organisation, he responded with the following:

> *Yes yes! And we provide the same benefits and features that you can benefit from public cloud but under our control I expect the information centre and the Kingdom here the size is big and the budget does allow us to build the business that is available abroad and keep the secrets of the data that is here* (P2NIC)

In the statement above there is a claim by the respondent that they can provide the same benefits of the public cloud, that the country is large and they have the budget to build a public cloud that is like that of foreign companies, but keep the data within the country.

There appears to be a contradiction in the understanding of the benefits of the public cloud, as stated in the literature the main benefit of the public cloud is that it takes advantage of scale and is offered at a very low cost in comparison to a private cloud, moreover, it takes away the burden and cost of establishing a cloud and is a readymade product.

6.7.2 Public Cloud Not Suitable for Saudi Government Use

One of the main ideas that arose from the interviews was the fact that a number of participants felt that the public cloud, as a cloud solution, was not suitable for the purposes of government. One of the participants who held the highest position for distributed systems in the National Information Centre which is the organisation responsible for government data especially that of a highly sensitive nature said the following about the public cloud:

> *we don't have any plans and this subject is not even discussed because we have concerns about the use of the public cloud for government in general and especially in the interior* (P1NIC)

The reference in the above to the 'interior' refers to the Ministry of the Interior which is responsible for a large amount of very sensitive data.

The same respondent was asked if these concerns could be alleviated by the presence of specialised employees in the cloud and he said the following:

> *this will ease the concern but still there will be shared resources in the cloud what we know is public cloud cannot provide full isolated segment or infrastructure especial for you, it will be shared resource and this the idea of the cloud in general so if there is resources it will ease the concern but still there will be concern because at the end of the day is public cloud so there are a lot of obstacles related to the security* (P1NIC)

The statement above there was concern that although having the presence of government employees in the cloud, there will still not be a fully isolated part of the cloud offered to government.

There was an amount of emphasis on the sensitivity of the data and that it should not leave the country for any reason, there was a certain element of expression that the data was not only sensitive in terms of being citizen data and there was a need to protect the privacy rights of citizens, but also that data of a national nature was very sensitive and its protection was necessary for the security of the country. In this case, the data should not go outside of the country. A senior official responsible for the government cloud made this clear in the following statement:

No. Sensitive data will not go out of the country or out of special data centre at all (P2NIC)

The information that this respondent was referring to was the data that was kept by the National Information Centre as this data. The idea that this data is highly sensitive and should not go out of the country is also expressed by another official at the NIC who said the following in response to a question about plans to use the public cloud for sensitive data:

I expect and according to my expectation and my experience at the centre the nature of the business at the centre doesn't allow data to go out of the centre because of the importance of the data and because of the sensitive of the information that we keep (P3NIC)

The idea of sensitive data not being able to be moved outside of the country was often expressed by the participants:

The public cloud like I said to you depending on the nature of the business there is secret data and sensitive data which are very difficult to get out of the country and I don't expect any country will allow it to get out of the country (P3NIC)

Some of the respondents said that if the security and privacy concerns were resolved then there would be consideration of the public cloud.

Another idea that arose in relation to trust was the fact that a number of the participants felt that the CSP would not understand the needs of the government departments.

Cloud providers are private organisations and most of their customers are also private organisations so how can we expect them to understand our needs as a government? (P2NIC)

The national information centre is responsible for policy about distributed systems which includes the cloud, and it was respondents from this organisation that were very concerned about the issue of the location of data.

6.7.3 Lack of Knowledge of Cloud Service Provider (CSP)

Not knowing who the CSP is or not having much knowledge or awareness of the CSP was a common theme in the interviews. One of the respondents was further questioned about the

reasons that they did not intend to adopt the public cloud for government use and in addition to the security concerns, one of the participants said the following:

> *data and services that are sensitive are locked at the public cloud and are operated by a company that we don't know or don't trust. Is it possible they provide enough protection or do they abuse the data which will affect the security side.* (P5CUST)

In the statement above the respondent is saying that the company that operates the cloud is an unknown entity which cannot be trusted, and either they could provide the protection that is required or they could abuse the data.

There was an indication that there was a high level of uncertainty about the cloud provider. In response to the question of whether participants perceived a positive reputation of their CSP there was the idea of not having enough information about their CSP:

> *I'm not sure about their reputation because I do not know enough about them, I would need more experience* (P10MOF)

Another respondent said the following:

> *I know who the company are and they do have a good reputation, but I'm not sure about their reputation for the cloud* (P12MOF)

This problem was also linked to a lack of dealing with the CSP. It is important to remember that although the organisations that are involved in this study did have a relationship with a CSP, it was either for the public cloud on a limited basis (i.e. non-sensitive data) or there was only consideration of the public cloud. Therefore, there was a limitation in terms of the extent and experience that they had with their CSP in relation to use of the public cloud.

Moreover, there was evidence that government officials who are responsible for decision made about the cloud had little dealing with international public cloud providers from around the world:

> *and if you mean security trust I can said we have some fears since currently who is leading the cloud service on this country is the biggest telecommunication companies which are they been target and frequently attacked from the hackers* (P7IMM)

From the statement in the above, it is important to note that the perception is that the public cloud in Saudi Arabia is provided by the largest local telecommunications providers, which are often targeted by hackers.

Another participant also indicated to the idea that there may be little or no dealing with international providers:

> *Depends where is data hosting, for government they prefer to host their data in any government premises for commercial (organisations) they prefer to host data inside country* (P11MOF)

In the statement above, where the government does use a commercial CSP it is not from outside the country because the government prefers to have data hosted inside the country. This idea agrees with the previous statement where there is an indication that the local telecommunications company is the provider of public cloud services in Saudi Arabia. More support for this idea that local companies would be preferable due to security and privacy concerns for sensitive data is found in the following statement;

> *of course the public cloud that comes with Window HP and Microsoft we don't have any plans and this subject is not even discussed because we have concerns about the use of the public cloud for government in general and especially in the interior* (P1NIC).

In reference to reputation, there was the idea that the participants depended on the experiences of other government departments in Saudi Arabia as well as the private sector.

> *The cloud provider that we use has been used by many different organisations in the government sector and we did not hear any issues about security* (P2NIC)

A number of the participants expressed the idea that they were not completely familiar with their CSP which increased the feeling of mistrust. Not knowing the CSP is a problem that has been highlighted in the literature (Huntgeburth, 2015) and a number of the participants expressed this idea of unfamiliarity. In response to the question about whether the participant trusted their CSP, one said the following:

> *It is difficult for me to say if I really trust the provider because I do not know them very well, and we are not considering the public cloud in the near future so we do not*

have much information about the provide and how they offer a public cloud service (P12MOF)

In reference to the different cloud concerns there was a high level of uncertainty among the participants. Uncertainty was found to be associated with different cloud factor which included security and compliance. Moreover, this uncertainty is often expressed as part of the relationship.

Im not sure about the provider and how they will offer us the security that we need, I don't feel that they understand how important security is for our ministry (P11MOF)

6.7.4 Dependency on Service Level Agreements

An idea that came up in the interviews was that there was a level of dependency on the SLA as a means to ensure that the CSP will do as they are expected to do. This idea was in response to the question that asked if participants trusted their CSP (question 4). An illustration of this idea was provided by the following respondent:

It is important to trust a CSP, we trust ours but they are local, however, I think that there should be assurances in the relationship and we can get that from the contract agreement that we have with them (P11MOF)

Moreover, one of the participants said that the SLA gave them a certain level of control in the relationship:

When you use the cloud you do not know where your data is and you do not know how it is managed which I think is big trust problem. The only way we can get any control about our data is with the service contract that we have with the provider (P2NIC)

In response to the question about whether participants felt that they could effectively negotiate with their CSP, there was an overall feeling that they felt that they could but this was in reference to negotiation of the SLA, one of the participants said the following:

Yes I can negotiate effectively with the cloud provider and it is not a problem for us to negotiate the agreement that we have between us (P5CUST)

Overall, there was a certain level of confidence in the CSP found in the agreement between them and government. Dependency on the agreement between the government and the CSP was also found in a statement about the perception of risk:

The relationship is governed by the agreement that there is between us and them, where I feel that there is a risk is where they do not follow that agreement (P3NIC)

6.8 Summary

The interviews revealed that the main area of concern was security and privacy and compliance with the law about the storage of sensitive data.

In reference to the relationship there were mixed perceptions about trust. As for negotiation, there were generally negative opinions about being able to negotiate with the CSP and the reason given for this was that government were concerned about the CSP understanding and servicing their requirements. The story was more positive for collaboration; however, it was often conditional on the CSP understanding government needs. Therefore, the concern about having needs understood is clearly evident.

The concern about government specific needs was reflected in other emerged themes in the interviews. Specifically, these concerns were reflected in the idea that government felt that the cloud was not suitable for government use and lack of knowledge about the CSP. These ideas reflect a sense of knowledge and certainty that the government have about the issue of using the public cloud, however, there was also some evidence that there was a lack of understanding of the public cloud.

7 Discussion

Objectives

- **Discuss the outcomes of the research**
- **Present implications in relation to other research**
- **Provide recommendations to CSPs**

7.1 Introduction

This study was based on the premise that in the investigation about trustworthiness in the cloud, studies were either focused on the cloud factors that affect trust such as security and privacy, compliance or governance (Aziz et al., 2013, Zwattendorfer et al., 2013, Haag et al., 2014, Nycz and Polkowski, 2015, Spiga et al., 2014, Hana, 2013), or they are focused on the relationship factors between the government and the CSP, for example trust and perception of risk (Huntgeburth, 2015, Ahmed and Hossain, 2014, Huang and Nicol, 2013, Burda and Teutberg, 2014, Ryan and Falvey, 2012, Ahmed and Hossain, 2014, Bochicchio et al., 2011, Baset, 2012, Zheng et al., 2014, Alruwaili and Gulliver, 2014). These studies in isolation do serve to offer, to a certain extent, an understanding of why government may be reluctant to use the public cloud. This study was based on the premise that both cloud and relationship factors are better considered together in order to understand government reluctance to adopt the public cloud. Therefore, the study offered a greater insight into the relationship and the cloud factors as concerns in that relationship. This is based on the idea that considering factors in isolation is weak and does not consider the full picture.

This idea leads to a concept on which the research design of the study was based. The research design and the methodology that was developed was simple; cloud factors as critical success factors combined with relationship factors as critical success factors applied in the research design to reveal reasons why government are reluctant to adopt the public cloud.

There is a symbiotic relationship between cloud factors and relationship factors, for example security as a cloud factor direct affects risk perception as a relationship factor, or relationship factors such as trust directly affects concerns about cloud factors such as compliance.

This consideration offered a more comprehensive view of the relationship where the interplay between cloud factors and relationship factors is better understood and shows that consideration of one type of factor in isolation would not serve to better understand the situation where a government is considering the public cloud. Moreover, this more detailed consideration of relationship and cloud factors has been justified by limitations in the literature. For example, Fan et al. (2014) do consider the cloud factors that are relevant to trust, and a number of these cloud factors are addressed, however, only trust is considered as if it is the only relationship factor that is relevant to cloud concerns.

It was one of the intentions of the study to help stakeholders in the government-CSP relationship, especially the CSP, to alleviate and overcome concerns through a more detailed and in-depth understanding of those concerns. With this in mind, the study considered not only the general cloud factors such as governance or security and privacy, but the specific areas, as potential areas of concern, within each cloud factor, considered as sub cloud factors.

Compliance and governance were areas that were shown to be of a particular concern for government because they have to adhere to their own, and international, laws and regulations regarding the management of citizen and government data (Hana, 2013, Diez and Silva, 2013, Hon et al., 2012). This would explain the high level of mistrust by government in these areas. Security and privacy and performance and offering are general requirements for all users of the public cloud and the literature has shown them to be especially a concern for government in relation to citizen data, however, this study has shown that there is a very high level of trust generally in these areas which is in stark contrast to the literature.

In reference to part of the first aim of the study, which states to reveal relationship factors within the government - CSP relationship that may have an impact on the government's intention to adopt the public cloud, the relationship values were tested alone and most did not offer an explanation for the reluctance of the Saudi government to adopt the public cloud. The government mostly trust their CSP and felt they could negotiate and collaborate with their CSP. However, the government did feel that they perceived a general risk with their CSP and they also perceived a negative reputation. The positive result for trust generally and negative result for reputation generally is further supported by the finding that trust was generally not linked to reputation.

7.2 Cloud and sub cloud factors and relationship factors

Where the relationship factors, which include trust, risk, negotiation, collaboration and reputation are considered against the various cloud and sub cloud factors, the results are varied for some relationship factors there were negative responses in relation to cloud and sub cloud factors, for example, there was trust in the CSP regarding performance and offering and a lack of trust regarding governance. However, it was not always the case that a lack of trust resulted in a lack of trust in the sub cloud factors. Here there is a discussion about the connection between relationship and cloud and sub cloud factors.

All of the relationship factors were analysed against each sub cloud factor of each cloud factor. The reason this analysis was carried out was to answer the second research question which was 'Are there certain cloud related factors that are affected by relationship factors that affect government confidence in the public cloud?'.

To provide an example of what the analysis was aiming to achieve, where negotiation was considered it was tested against a cloud factor such as security to determine if the government felt if they could negotiate for security and privacy. Furthermore, negotiation is then analysed against the sub cloud factors of security and privacy, for example, *Assurance regarding CSP employees.* Therefore, the results of this analysis will show which areas of the cloud are affected by relationship factors, for example, government may be reluctant to adopt the public cloud because they feel they cannot negotiate for *assurance about the CSP employees* in relation to security and privacy.

One of the main ideas that arose from the results was that there was a very significant difference in the results for the cloud factor and the results for the associated sub cloud factors, this was the case for most of the relationship factors and cloud factors. Responses to the cloud factors for most of the relationship factors were strong one way or the other, the respondents were sure how they felt about the link between the relationship factor and cloud factor. Where the respondents where then asked about the sub cloud factors within each cloud factor the results were either completely opposite to the results of the associated cloud factor or the results were polarised among the different sub cloud factors.

7.2.1 Governance

There was agreement with the idea that government trusted their CSP, however, this was in response to a general feeling of trust, where governance as a cloud factor was mentioned then the level of trust significantly decreased to the extent that the majority said that they did not trust the CSP, this was also found to be the case for compliance.

The literature has shown that of particular concern for government is that they gain a certain level of governance over data and systems in order to have confidence in the public cloud (Mreea and Munasinghe, 2016; Haag et al., 2014; Craig et al., 2009). This has also been shown to be something that is necessary in order for a government to be compliant.

Specifically, within governance the sub cloud factors where there was a lower level of agreement or more negative perception were *Control and knowledge over CSP employees,*

Dynamic SLA, Knowledge and control over third party issues and *Assurance about other cloud tenants*. This was found to be the case for trust whereby respondents did not trust their CSP in these areas, and a corresponding negative response was found for risk whereby respondents perceived a risk. Moreover, where respondents were asked about their ability to negotiate generally with their CSP they also felt that they could not for these sub cloud factors of governance, and the same was found to be true for the ability to collaborate generally.

This idea is then further supported by the fact that for these sub cloud factors for governance there was a low perception of a positive reputation. The idea that there are sub cloud factors that would be considered a particular concern for government, even before the research was carried out, is further supported by the fact that for more general sub cloud factors that would be a concern for all organisations, there was less of a concern. In other words the government felt that they could trust, perceive less risk, negotiate, collaborate and perceive a positive reputation in more universal sub cloud factors such as *Auditing and measuring the CSP* and *sufficient notice of disruption* which are common provision in SLAs. A negative reputation for governance was found to be correlated with a negative perception of being understood for governance requirements, which may further explain the reluctance to adopt the public cloud.

7.2.1.1 Clarity of roles and responsibilities

This was a sub cloud factor of governance for which there was a high level of trust, a low perception of risk, a high perception of the ability to negotiate, a perception that requirements are understood, a perceived ability to collaborate and a perceived ability to communicate. However, there was a perception of a negative reputation of the CSP for this sub cloud factor. This has implications for CSPs that they have to address why they have a poor reputation in this area. These concerns agree with the concerns about governance found in the literature (Haag et al., 2014, Nycz and Polkowski, 2015, Diez and Silva, 2013). It is important to note, as part of a wider theme in the findings, *clarity of roles and responsibilities*, is often a standard provision in SLAs, and not considered a government-specific concern.

Who is responsible for what both on the side of the government and the CSP is important for an overall effective relationship and functioning of government in the cloud. The positive findings for this sub cloud factor show that there is a possibility for an assurance framework to ensure a clear governance strategy where benefit can be achieved in the cloud (Rebollo et al., 2012).

7.2.1.2 Need for knowledge and control over data and processes

This sub cloud factor was important because it is an essential part of governance. The literature review has shown that government need a certain level control and knowledge over data and processes in the cloud (Norr et al., 2016, Brender and Markov, 2013, Firdhous et al., 2011, ENISA, 2011, Kanwal, 2014). There was almost equal trust and mistrust for this sub cloud factor but with a perception of risk. However, the government did strongly feel that they could negotiate for this area despite the fact that they felt that the CSP did not understand their requirements as part of the negotiation process. Moreover, despite the fact that they felt they could negotiate, they did not feel they could collaborate in this area. Unfortunately, collaboration has been cited in the literature as a remedy for the loss of governance over data (Rebollo et al., 2012). There was a high level of uncertainty regarding the CSP's reputation in this area.

The perception of risk is understandable given the fact that detailed monitoring of cloud systems by the cloud consumer is not something that is offered in most SLAs (Jansen and Grance, 2011).

7.2.1.3 Assurance about other cloud tenants

The government was concerned about other tenants that share the public cloud, however, despite these concerns, government felt they could negotiate this area despite the fact they felt the CSP does not understand their requirements or that they could collaborate. A poor reputation was also perceived for this sub cloud factor. It is reasonable that government are concerned while at the same time having the ability to negotiate. According to Almorsy (2011) because of multitenancy in the cloud, each party has their own Security Management Process (SMP) that they want to enforce in the cloud, this would explain the government perceived ability to negotiate. However, because no one single tenant has the full security picture there is significant loss of governance (Almorsy, 2011).

7.2.1.4 Knowledge and control over third party issues

Third parties include any party other than the CSP that are involved in providing the technology for the provision of the cloud. The most obvious example is the cloud provider (CP) which provides the physical infrastructure of the cloud. The results were mostly negative for this sub cloud factor, the government did not trust the CSP in terms of the idea that they will be given an acceptable level of knowledge and control over third parties, they perceived a high risk, they felt they could not negotiate and that the CSP would not

understand their requirements during that negotiation, there was a strong perception that they could not collaborate and they also perceived a poor reputation. Brenda and Markov (2013) say that concerns about employees of the CSP should extend to the cloud provider as well. The lack of trust by the government is made understandable by the fact that between the CSP and the CP and the government as a customer, there are different ideas about what governance is (Firdhous et al., 2011) which would explain the concerns about negotiation, collaboration and reputation.

7.2.1.5 Dynamic SLA

A dynamic SLA was something that was identified in the literature as something that would be important to government when considering the cloud (DiModica, 2014, Kanwal, 2015, Filiali and Yagoubi, 2015) and is important especially in consideration of the fact that SLAs are often standard and would not be suitable to meet the complex and ever changing requirements of government. This issue was reflected in the responses by government where there was a perceived high level of mistrust and risk, the perceived inability to negotiate and have requirements understood, the perceived inability to collaborate and the perception of a poor reputation in this area. Much like other sub cloud factors that received negative responses, a dynamic SLA was a government-specific concern.

7.2.1.6 Control and knowledge of CSP employees

There were negative responses regarding this sub cloud factor, the government strongly mistrusted the CSP and perceived a high level of risk about this sub cloud factor. Moreover, the government felt strongly that they could not negotiate for this sub cloud factor. The findings of this study confirm the concerns that have been put forward by Brenda and Markov (2013) and the CSA (Cloud Security Alliance) who say that the employees of the cloud are a major consideration for government and governance. This idea is further supported by an idea that arose in the interviews that the government lacked knowledge about their CSP.

7.2.1.7 Auditing and measuring of CSP

The government trusted the CSP that they would be allowed to audit the CSP for governance, however, they perceived a level of risk. This is particularly relevant to the government as the public sector where governance requires internal and external auditing (Craig et al., 2009). Moreover, due to the nature of the public cloud where data is geographically dispersed,

enforcement becomes difficult (Craig et al., 2009). However, the government indicated that they were not concerned that there would be auditing and measuring the CSP for governance issues. Again this is a sub cloud factor that is included as a standard provision of SLAs.

7.2.1.8 Governance during migration

There was very little concern about governance during migration, evidence by a high perception of trust and risk. Migrating to the cloud is a process that is well-established and CSPs have experience of this, and is also well established in SLAs. This shows that the government feel they will have a certain level of control and involvement in the migration process.

7.2.2 Compliance

Continuing with the idea that there are certain sub cloud factors that are of a particular concern for government in comparison to other sub cloud factors, looking at the sub cloud factors of compliance there was a deviation from this idea as far as trust and risk are concerned. It is important to note that compliance and its sub cloud factors are obviously a concern for government generally, however, for *Clarity and confidence about jurisdiction* there was very little concern for trust and perception of risk and for negotiation there was a very high level of confidence. However, for risk, trust and negotiation there was a high level of concern about the location of data, whereas for collaboration there was a high level of confidence. In addition to these ideas, the government perceived a poor reputation for all the sub cloud factors of compliance except for *Compliance when migrating.* Overall this shows that as far as compliance is concerned there is no clear pattern that suggests that the government is specifically concerned about sub cloud factors that would be a particular concern to government, the real problem for compliance is, however, reputation which has implications for the CSP to consider.

7.2.2.1 Continuous auditing and assessment

Compliance is an essential requirement for government and they need compliance to be continuously audited and assessed. Although there was a negative perception in terms of risk and trust, there was some agreement. The government were confident that they could negotiate for this area but did feel that the CSP did not understand their requirements. Moreover, there was a strong agreement with the idea that they could collaborate for this sub cloud factor, and although they generally perceived a poor reputation, around a quarter did

perceive a positive reputation. The mixed opinions for this sub cloud are understandable in light of the fact that it has been claimed by Ahmad and Janczewski (2011) that the CSP may not be able to comply with auditing requirements because of the laws in their own jurisdiction. Moreover, Craig et al. (2009) said that the public sector faces legal challenges for auditing, which is made more difficult by geographic dispersion.

7.2.2.2 Clarity and confidence about jurisdiction

Government were very sure they could trust their CSP in this area and there was a low perception of risk. They felt positive they could negotiate and collaborate, but despite these positive findings they did perceive a negative reputation for this sub cloud factor. These findings are contrary to most of the literature that is about the issue of jurisdiction raises concerns. These concerns include issues related to citizen data being located in another country (Ahmad and Janczewski, 2011), uncertainty about the laws of which jurisdiction would apply and the government requirement to comply with national and international legal and regulatory frameworks (Han, 2013). Furthermore, the benefits of cloud computing for government can be undermined if geographic borders become fractured (Bhatt, 2012). Given these numerous difficulties identified in the literature, the government were not concerned about this sub cloud factor of compliance.

7.2.2.3 Data management

The results for this sub cloud factor reflected those for the previous sub cloud factor. In summary, there were positive perceptions related to trust, risk, negotiation and collaboration, while at the same time a negative perception of reputation. So for data management although there was a negative perception of the CSPs' reputation, it did not affect their trust or perception of risk or the ability to negotiate and collaborate with the CSP.

7.2.2.4 Roles and responsibilities for compliance

In order to achieve compliance there needs to be clarity about who is responsible for what aspects of compliance. There was strong disagreement that the government could trust the CSP, and there was a high perception of risk in this area. This was reflected in the negative perceptions for the ability to negotiate and collaborate as well as a perception of a negative reputation. These negative perceptions by government reflect the issue raised by Hon et al. (2012) who said that the role of CSPs in compliance is not understood by CSPs and is ill defined, moreover, CSPs do not give much attention to regulatory or legal implication

because negotiated terms are often standardised. Here, therefore, there is another problem associated with standardised contracts which are clearly affecting the government's willingness to adopt the public cloud. Other results for other sub cloud factors also suggest standarisation of agreements is a problem for government.

7.2.2.5 Security and privacy

Security and privacy towards being compliant has been shown to be important to government. Although government were generally positive about trust and risk, there was a level of uncertainty. There were mixed opinions about the ability to negotiate, but negative perceptions about the ability to collaborate and a negative perception of a reputation in this area.

7.2.2.6 CSP ability to be compliant

There was a high level of skepticism for this sub cloud factor, there was lack of trust, a concern about risk and a perception of a poor reputation, however, the government did feel that they could collaborate in this area. In relation to this, there is a recurring theme found in this study that despite negative perceptions about cloud and sub cloud factors, the government still felt that they could negotiate and collaborate. This is more reflective of the abilities of the government once a relationship with a CSP has been established, however, it is the lack of trust and the perception of risk and poor reputation in relation the CSP that is the impediment to adopting the cloud in the first place.

7.2.2.7 Data location

It is important for government to be aware of where their data is located as part of achieving compliance. The government are accountable to their public and therefore, should be aware of the data's location at any time. Although they could not trust the CSP and did perceive a risk, there were some positive perception for risk and trust. Although the government felt they could not negotiate for data location, which is something that takes place before an agreement is made, they did feel they could collaborate, something that takes place during the relationship. As for the reputation, there were mixed opinions. Similarly, problems have been identified in the literature which include user concern about geographic location of data (Hon et al., 2012) and public organisation uncertainty about jurisdiction and compliance at a global level.

7.2.2.8 Compliance when migrating

Compliance during migrating was not a concern for government, where all relationship factors were found to be positive, in particular the perception of the ability to negotiate for this sub cloud factor. The process of migrating to the cloud does not cause a concern for government. This is a surprising issue because it is during migration to the cloud where data is vulnerable and it has been shown in the literature to be an aspect of the adoption of the cloud that a government have to be ready for (Kurdi et al., 2011) and involves a number of steps (Singh, 2012). Therefore, an explanation is that government trust the CSP competence in this area. Moreover, as with other sub cloud factors where there is less concern, compliance during migration is found in SLAs as standard.

7.2.3 Security and privacy

The literature has shown that security and privacy is one of the main concerns of government not wanting to adopt the public cloud, however, this study has shown that there is a high level of trust generally for security and privacy. This requires a rethink of assumptions that are made in the literature, that may not be appropriate to the specific situation of government considering the public cloud. Where respondents were questioned in relation to the sub cloud factors of security and privacy there was a clear expression of the idea that there are specific sub cloud factors, which would be expected to be a particular concern for government, where there was a high level of concern, this concern for these sub cloud factors was found to be true for trust, risk, negotiation, collaboration and reputation. Particularly, there were strong opinions about *Security related to third parties, Tailored security and privacy policy, Assurance regarding CSP employees* and *Clarity of roles and responsibilities* whereby the respondents expressed strong negative perceptions in the areas of negotiation, collaboration and reputation in particular. This was in contrast to the other sub cloud factors that received a more positive response from the government.

Therefore, in terms of trusting the CSP, having no perception of risk and having the ability to negotiate and collaborate, there were negative opinions for specific sub cloud factors of security and privacy considered a particular concern for government, a recurring theme of this study. This clearly shows that these sub cloud factors are major inhibitors for adopting the public cloud. This was also evident in the interviews where although there were generally positive attitudes about collaboration, there were real concerns about collaborating for the security and privacy of sensitive government and citizen data.

However, in reference to security and privacy generally there were positive responses for all relationship factors, this has been a recurring theme of this study, that the initial responses to cloud factors are often different to the responses for certain sub cloud factors, where there seems to be an initial confidence and positive response for the cloud factor, this is met with more skepticism and negative responses for some of the sub cloud factors.

As part of their perceived ability to negotiate, the government felt very confident that they could specify their security and privacy requirements. Again, this is a standard expectation of information security management systems that the cloud customer should be able to specify their security requirements on the cloud hosted assets (Almorsy, 2011). Moreover, in addition to be allowed to specify security requirements as part of ISO27000 requirements for a security management system, customers should also be allowed to continuously monitor asset security and policy that should be based on security policy that the cloud customer already uses. Therefore, the nature of international standards for security management systems in the cloud acknowledges that the customer is very knowledgeable about their own security requirements.

7.2.3.1 Security related to third parties

For all of the relationship factors in association with this sub cloud factor there were negative responses. Concerns about third parties was also found to be an issue within governance. This was found to be one of the main concerns for government in consideration of moving to the cloud, the reasons for which have been presented in governance above in the previous section. This high level of negativity is understandable given that governments are particularly concerned about the deployment of sensitive data, it has been shown that in relation to third parties, such as the CP, storing sensitive data is a particular concern for government (Alshomrani and Qamar, 2013). This is the reason for governments often opting for private clouds in order to store data because of these security concerns (Bhatt, 2012, Khan et al., 2011).

7.2.3.2 Monitoring of policy adherence

The government were very positive about this sub cloud factor, there was a very strong level of trust and an associated low level of risk perception. Overall there were no concerns about the CSP monitoring their adherence to their security policy. Therefore, this was not a factor that negatively affected the government's d ecision to adopt the cloud. It is in fact a standard expectation of information security management systems that a CSP should adhere to their

security management standards and continuously monitor, evaluate and improve information security on a regular basis as part of requirements for international standards (ISO 27000) (Almorsy, 2011). This is an assurance that is offered as standard as part of internationally recognised and required standards for the cloud, and it is thus understandable why government have no relationship concerns for this sub cloud factor.

7.2.3.3 Sufficient involvement in security

Although there was some trust here, there was also some perception of risk. The government felt they could both negotiate and collaborate to be involved in security. It is important in order for government to achieve both governance and compliance to be sufficiently involved in security, the literature has shown that they need to very involved and be able to fully liaise in this area. Again, sufficient involvement in security by the customers is something as standard in security management frameworks for the cloud (Almorsy, 2011). However, it is also understandable that a government would require a higher level of involvement in the cloud that is currently offered.

7.2.3.4 Tailored security and privacy policy

This was found to be a government specific concern. As with other sub cloud factors that are related to the idea of a tailored service, there is need for government to be afforded a tailored service in security and privacy. One of the main concerns for government is the well-known characteristic of public cloud services which is that they are standardised, which is necessary for their economies of scale and affordability. There were strong negative opinions about this sub cloud factor, there was a strong lack of trust and a perceived inability to negotiate and collaborate, and understandably a perception of a poor reputation as the public cloud is known for being standardised.

7.2.3.5 Clarity of roles and responsibilities

The government did not trust the CSP to be clear about who is responsible for which aspects of security and privacy. There was lack of trust and a high perception of risk, although there were mixed feelings about the ability to negotiate and collaborate and the reputation of the CSP for this sub cloud factor. Assuring clarity for roles and responsibilities between the government and the CSP is a requirement for managing security risks and ensuring that the government's security requirements are met (Jansen and Grance, 2011), and the doubt that was shown in this study for this area is clearly a reason for reluctance to adopt the public

cloud. Moreover, when the government move to the cloud roles and responsibilities are no longer the same as they were in the traditional computing environment (Jansen and Grace, 2011). Therefore, this uncertainty understandably leads to the high perception of risk found in this study. Another cause of risk perception associated with a lack of clarity for roles and responsibilities for security is the separation of duties. This refers to dividing roles and responsibilities in order to ensure that no single individual has the power to subvert critical processes (Microsoft and Estonia Ministry of Economic Affairs and Communications, 2015).

In reference to the relationship factors, the association here between risk and trust is understandable, however, there were a significant number of government respondents who felt they could negotiate and collaborate for clarity for roles and responsibilities. This can be due to the fact that they are already knowledgeable about roles and responsibilities for security and privacy and that clarity for these roles and responsibilities is required for success in the cloud (Jansen and Grace, 2011).

Therefore, it is not their perceived ability to negotiate and collaborate that is an impediment to public cloud adoption, but instead their perception of mistrust and risk. To a large extent, the government have control over their perceived ability to negotiate and collaborate, so the more positive responses for these relationship factors can be explained by this level of control, whereas for trust, risk and reputation this is not in the control of government.

7.2.3.6 Assurance regarding CSP employees

A government is responsible to its citizens about the protection of data, therefore, they should be assured about the employees of the CSP that they do not have bad intentions towards the government. Naturally this was a significant concern for the government evidenced by strong negative responses for all relationship factors. Therefore, this is a clear reason for the reluctance by the government to adopt the public cloud. Malicious insiders has been cited as one of the main security risks for the public cloud (Venkatraman, 2014).

Specifically, the results of this study show that there was a very strong negative perception of the ability to negotiate for this sub cloud factor. However, it has been shown that negotiation for security and privacy for government in the public cloud is necessary and includes negotiation for vetting employees as a main concern (Jansen and Grace, 2011). The strong inability to negotiate for this sub cloud factor would also explain the associated strong perception of risk.

7.2.4 Performance and offering

In consideration of the sub cloud factors of performance and offering a similar idea was also found as for security and privacy. For the sub cloud factors which included *Customisable cloud environment*, *Dynamic / flexible SLA*, *Meet government specific requirements* and *Additional specialised staff for government needs* there were negative perceptions for all of the relationship factors. In other words, there was a lack of trust, a perception of risk, a perception of the inability to negotiate and collaborate and a negative perception of reputation for these cloud factors.

Overall, the results have revealed that where there is negative opinion about the relationship factors it is mostly related to those sub cloud factors that are of particular concern for government. The reason that these sub cloud factors have been considered to be a particular concern or relevance to government is because it has been suggested by the literature. This study included these sub cloud factors not only to test to test if they are a concern for the Saudi government and adoption of the public cloud, but also to reveal the link between relationship factors and these sub cloud factors. It can be said therefore, that there is a lack of trust, a perception of risk, an inability to negotiate, an inability to collaborate and a negative perception of reputation for sub cloud factors, for most cloud factors, that are shown in the literature to be a particular concern for government.

7.2.4.1 Customisable cloud environment

In reference to the problem of standardisation of public cloud services and it being a cause of concern for government, there was a strong sense of mistrust, a high perception of risk and a perceived inability to negotiate for a customisable cloud environment. There are a number of sub cloud factors that are associated with the idea of moving away from a standardised service to a more tailor-made or customisable cloud service, these include a *Dynamic SLA*, *Tailored security and privacy policy*, *Meet government specific requirements* and *Additional specialised staff for government needs,* all of which received negative responses for most relationship factors.

This study has shown that there was a very strong negative perception of the ability to negotiate to this sub cloud factor. Not being able to negotiate would be detrimental for achieving a customisable cloud environment, especially in large and regulated organisations such as governments whereby negotiation would have to be increased in order to make sure

that government requirements are met (Hon et al., 2012). This would therefore explain the overall negative responses for this sub cloud factor, especially, the perception of risk.

It is important to note, however, that it is not just the inability of the government to negotiate for a customisable cloud environment that is the only impediment to cloud adoption, there was also a high level of mistrust of the CSP for this area. Therefore, the government, through their responses, suggest that it is both the fault of the CSP and the government that the issue of not being able to achieve a customisable cloud environment is the cause of reluctance for public cloud adoption.

7.2.4.2 Dynamic SLA

Another sub cloud factor relevant to the problem of standardisation is Dynamic SLA, whereby the government require an agreement that is flexible and dynamic according to the ever-changing requirements. The government also felt strongly about this issue where there were strong negative responses for all of the relationship factors. Again, it is the perceived inability by the government to negotiate that is a cause for concern here, because according to DiModica (2014) the inability to achieve a differentiated cloud service is the result of poor negotiation. This sub cloud factor is considered a particular concern for government because it is an absolute requirement of government that they have flexibility in their agreements which in turn maintains trust between the parties (Kanwal, 2014) and the results have shown that the government have no confidence in themselves or the CSP for this issue.

7.2.4.3 Continuous monitoring of performance

Although there was some uncertainty about trusting the CSP that they would continuously monitor their performance, they mostly trusted their CSP in this area. Despite there being little perception of risk, there were some who did perceive a risk. Moreover, what was noticeable about this sub cloud factor was the very strong perception of the ability to negotiate. This sub cloud factor is closely related to *Auditing and measuring of CSP, Continuous auditing and assessment* and *Monitoring of policy adherence,* as sub cloud factors from other cloud factors, where a very positive perception of the ability to negotiate was also found. Again, these are standard provisions in current SLAs which would explain the positive perception by the government of the ability to negotiate.

These sub cloud factors are something that take place on a continuous basis and therefore, the ability to collaborate for these areas is relevant. For this sub cloud factor, there were mixed

opinions about the ability to collaborate, although there were marginally more who were confident to collaborate for this area. For all of the other similar sub cloud factors, mentioned in the previous paragraph, there was a strong positive perception of the ability to collaborate. Therefore, continuous monitoring of performance as a sub cloud factor of performance of offering, and the other closely related sub cloud factors from the other cloud factors, the associated ability to collaborate and negotiate for these sub cloud factors, and a positive perception of trust and low perception of risk, suggest that these are not reasons for reluctance of government to adopt the public cloud, especially as they can collaborate on an ongoing basis which is a requirement for achieving these sub cloud factors.

7.2.4.4 Meet government specific requirements

Again, this sub cloud factor is associated with the problem of standardisation. There was a very high level of skepticism for this sub cloud factor, the government did not trust the CSP and perceived a very high risk. Moreover, the government felt that they could not negotiate or collaborate for this sub cloud factor and they perceive a very negative reputation. Meeting government specific requirements is closely associated with other sub cloud factors where there is consideration of government specific needs, these include *Tailored security and privacy policy*, *Customisable cloud environment* and *Additional specialised staff for government needs.* These have been shown to be of particular concern for government. Therefore, the perception of government that they cannot achieve these requirements, either through their own perceived inability, or a perceived inability of the CSP, is a significant factor in reluctance to adopt the public cloud. This is part of an overall theme that has emerged in this study, that the main inhibitors to public cloud adoption are factors that would especially be a concern to government, this is in contrast to factors that are often standard for which the government has less concern. This issue is discussed in more detail in section 7.4 below.

7.2.4.5 Additional specialised staff for government needs

Government performance requirements for the cloud would be more numerous and complex than it would for other types of organisation. There is a need for specialised and dedicated staff within the CSP to support these needs. In light of this, there was a very strong concern about this sub cloud factor, this was in terms of trust, risk, the ability to negotiate and collaborate and a very poor perception of reputation. This was a sub cloud factor that was considered a particular concern and relevance for government. It has been suggested that the

nature of the cloud, in terms of its scale, does actually allow cloud staff to become specialists in different areas of the cloud because the scale of the cloud allows staff to be free from other duties (Jansen and Grace, 2011). Given that there is a lack of trust and a poor reputation of the CSP, it would be beneficial for the CSP to inform the government about the potential for specialised staff.

7.2.4.6 Back-up and recovery

Back-up and recovery is an important issue for government, especially in the case of an attack both cyber and physical. This is a service that is offered as standard in agreements with public cloud providers. In reflection of this, the government were positive in terms of trust and risk, however, there were mix responses about negotiation for this sub cloud factor.

7.2.4.7 Sufficient support lifecycle

Despite the negative view that the CSP will meet government requirements or offer additional specialised staff, the government did feel that the CSP would offer a sufficient support lifecycle, this could be because this is a well-known offering that is found in current SLAs.

7.2.4.8 Sufficient notice of disruption

There was a mixture of perceptions of trust that there would be sufficient notice of disruption, but despite this there was a generally positive view of this sub cloud factor. Again, notice of disruption is something that is offered as standard and the government will be aware of this, this is reflected in the positive response for this sub cloud factor.

7.2.4.9 End of relationship

Overall, for all relationship factors there was a positive perception of this sub cloud factor. The closely related sub cloud factor of *Sufficient notice of disruption* also revealed a positive response. The termination of a service is something that is clearly stipulated in the SLA, and therefore, the government have little concern about these areas.

7.3 Relationship factors with other relationship factors

Relationship factors were analysed against other relationship factors in order to find out how they affect each other, a simple example is the interplay between trust and risk perception. These ideas were based on theory that suggest that there is interplay between relationship

factors (Burda and Teutberg, 2014, Ryan and Falvey, 2012, Alshomrani and Qamar, 2013, Abbadi and Alawneh, 2012).

7.3.1 Trust with other relationship factors

Trust was correlated with other relationship factors in order to determine if there is a correlation between them, this was done against the cloud and sub cloud factors, to see for example, if trust in governance corresponded to an ability to collaborate for governance, or if a perception of risk in compliance was correlated with trust for compliance.

7.3.1.1 Negotiation

The various relationship factors were analysed to see if there were correlations between them. This offers an explanation of how the interplay between relationship factors affect the decision to adopt the cloud. In reference to negotiation and trust, the analysis was carried out to identify a correlation between the two, in order to determine if trust, whether high or low, had an effect on the perception of the ability to negotiate. This correlation was determined for each cloud and associated sub cloud factor in order to provide further insight into how trust and the perceived ability to negotiate relate to specific areas of the cloud. For example, a higher level of trust may increase the perceived ability to negotiate for governance but not for security and privacy, or a low level of trust may only affect the perceived ability to negotiate for compliance.

There was a positive correlation between negotiation and trust found for compliance, security and privacy and performance and offering which suggests that where there is trust, the government perceive that they can negotiation for these areas of the cloud. However, for the specific sub cloud factors the story was different.

Although correlations were found between trust and the perceived ability to negotiate for five of the eight sub cloud factors of compliance, these correlations were generally weak, the strongest correlation was found for roles and responsibilities where there was a moderate correlation. Therefore, for compliance and sub cloud factors for compliance trust does not have a significant impact on the ability to negotiate compliance requirements.

For trust in security and privacy and the ability to negotiate security and privacy, there were only two sub cloud factors where a significant correlation was found, namely; *tailored security and privacy policy* and *clarity of roles and responsibilities*. This means that for all of

the other sub cloud factors there was no correlation between trust and negotiation. Therefore, there was very little relationship found between the perception of trust and the perceived ability to negotiate for security sub cloud factors. In fact the weakness in this correlation was more profound for security and privacy than for other cloud factors.

In relation to performance and offering there was also a positive, however, weak correlation between the perception of trust and the perceived ability to negotiate. For four out of the nine sub cloud factors for performance and offering there was a correlation found.

It is important to note that where there was a correlation between perception of trust and the perceived ability to negotiate it was in relation to areas of the cloud that are considered a particular concern for government. Specifically, correlations were found for customisable cloud environment and Dynamic SLA, both of which are requirements for government.

7.3.1.2 Collaboration

The correlation between trust and collaboration was designed to see if there was a relationship between the perception of trust and the ability to collaborate. Collaborate refers to the working relationship once an agreement has been made. The results show a moderate correlation between these two relationship factors for governance. This means that trust is moderately related to collaboration as far as governance is concerned.

This correlation was also found for five out of the eight sub cloud factors of governance. It is important to note that these sub cloud factors are of a particular concern to government. The strongest correlation was for the need to have control over data and processes, followed by other government concerns including assurance about other cloud tenants, knowledge and control over third party issues, control and knowledge over CSP employees and auditing and measuring of CSP.

The correlation between trust and collaboration was found to be stronger in relation to compliance where a strong positive correlation was found. However, upon further investigation into the sub cloud factors of compliance, the correlations were mostly weak and non-existent. This was also the case for security and privacy where only two sub cloud factors had positive correlations; *tailored security and privacy policy* and *clarity of roles and responsibilities,* albeit moderate correlations. Because the frequencies show that for both trust and collaboration there was a generally negative agreement in relation to clarity and confidence about jurisdiction, this means that where the government do not trust the CSP

they also feel that they cannot collaborate where clarity and confidence about jurisdiction is concerned. It is important to note that jurisdiction is an issue that government is concerned about, the literature has shown that concerns about jurisdiction are one of the reasons governments are reluctant to use the public cloud.

For the performance and offering sub cloud factors there were moderate positive correlations found between trust and collaboration for *Dynamic / SLA* and *Additional specialised staff for government needs*, both of which are of specific concern for government. In reference to Dynamic SLA specifically, for both trust and collaboration there was a high level of disagreement, therefore, there is a link between where the government do not trust the CSP and where they feel they cannot collaborate with the CSP in the area of a Dynamic SLA. The literature has shown that one of the main problems with a public cloud is that the SLAs are often standardised (Hon et al., 2012, Baset, 2012, Burden, 2014, Di Modica and Tomarchio, 2014). This study has shown that there is a lack of trust about dynamic SLAs and an associated lack of the perception of the ability to be able to collaborate about dynamic SLAs.

In reference to the additional specialised staff for government needs, this is something that has been shown to be important to government and gives them more confidence, moreover, this would allow for more governance and increased compliance. The results show that the government did not trust the CSP in regards this sub cloud factor and they also disagreed with the idea that they could collaborate in this area, this was evidenced by the moderate correlation between the two.

7.3.1.3 Reputation

The link between trust and reputation has been established in the literature (Huntgeburth, 2015, Almanea, 2014, Fan and Perros, 2014). There was a correlation between trusting the CSP and a positive perception of reputation for the governance cloud factor. The results showed that the government did not trust the CSP in relation to governance and the vast majority disagreed with the idea that they perceived a positive reputation in relation to governance, and the two were positively correlated.

This was also found to be true for compliance where a strong correlation was found between trust and perception of a positive reputation. A majority of respondents said that they did not trust the CSP in relation to compliance with a corresponding majority of respondents not agreeing with the idea that they perceive a positive reputation.

Sub cloud factors where there were moderate correlations between trust and reputation are areas that would be of particular concern for government and they included *Roles and responsibilities for compliance* and *CSP ability to be compliant*. There was no correlation found for *Clarity and confidence for jurisdiction* which is an area that government would be expected to be concerned about.

For both trust and perception of a positive reputation there was a very high level of agreement in relation to security and privacy. The fact that there was a high level of trust in security and privacy shows that this is not the reason that the government have for not adopting the government cloud, moreover, it shows an associated strong perception of reputation in this area would also not be a reason for reluctance. However, this is security and privacy generally, and where the sub cloud factors of security and privacy are considered then this reveals that there are concerns, this is the case for both trust and reputation.

Upon examination of the sub cloud factors of security and privacy, and the associated correlation between trust and reputation, it was shown that only two of the sub cloud factors positively correlated, these included *Clarity of roles and responsibilities* and *Assurance regarding CSP employees*. It is interesting to note that for *Clarity of roles and responsibilities* there was a strong positive correlation, this means that where the government trust the CSP they also perceive a positive reputation in relation to *Clarity of role and responsibilities* and where they mistrust about CSP employees there is an associated poor reputation. This has implications for the CSP, if they want to increase or maintain trust in the relationship they have to improve or maintain their reputation in these areas.

There was no correlation between trust and reputation in reference to performance and offering as a cloud factor, meaning that a general trust in performance and offering did not result in a positive perception of reputation as far as performance and offering is concerned. However, the results were different when looking at the sub cloud factors. It is interesting to note that of the sub cloud factors for performance and offering where a positive correlation was found, they were all areas that would be particularly important to government and the include a *Customisable cloud environment, Dynamic / flexible SLA, Meet government specific requirements* and *Additional specialised staff for government needs.* Therefore, it is important for the CSP to improve and maintain their reputation in areas that are not normally offered in standard SLAs.

The frequencies for these sub cloud factors reveal the following: for *Customisable cloud environment, Dynamic / flexible SLA* and *Meet government specific requirements* there was a high level of disagreement for both trust and reputation and for *Additional specialised staff for government needs*, there was a strong level of disagreement for both trust and reputation. Therefore, these results confirm that governments do not trust their CSP in relation to these areas which are evidently particular concern for government, and there is a corresponding lack of a positive reputation for the same areas.

Having sufficient information about the CSP is associated with reputation. The results show that there was little correlation between trust and having sufficient information about the CSP. This was the case for the four cloud factors. Specifically, there was little correlation for governance, no correlation for compliance, only a weak correlation for security and privacy and no correlation for performance and offering. In reference to the sub cloud factors for all cloud factors except performance and offering, there was very little correlation. For performance and offering most of the sub cloud factors did correlate. This means that the level of trust that the government has in their CSP is not associated with the amount of information that they have about the CSP for most of the sub cloud factors.

Therefore, the finding here seems to be contrary to the literature, where not only is it suggested that information about the CSP is something that has an influence on the decision to adopt the public cloud, but also there are mechanisms in place which include organisations that are dedicated to collecting information about CSPs towards allocating them a level of trustworthiness which is used by potential customers of the public cloud.

Where trust was examined for its influence on, or being influenced by, other relationship factors, it was found that this influence or connection was prevalent for sub cloud factors that were a particular relevance to government. So, trust, negotiation, collaboration and to a certain extent reputation, have influencing effects on each other where government-relevant factors are concerned. Given that the general results for these government-relevant sub cloud factors are often negative, a negative perception of trust will lead to a negative perceived ability to negotiate and collaborate and vice versa.

This is one of the main findings of the study, that sub cloud factors that are particularly relevant to government are perceived negatively by government, not only as evidenced here where relationship factors are analysed against other relationship factors, but also when relationship factors are analysed against sub cloud factors.

7.3.2 Risk with other relationship factors

It would be fair to say that where there is a correlation between perception of risk and collaboration, this tells us that where there is a perception of risk there may be the inability to collaborate, and vice versa. But it is important to know if this is true for security and privacy and the sub cloud factors of security and privacy. In other words, if there is a perception of risk for security, is there a corresponding lack of confidence to collaborate on security?

There was a high level of a perception of a risk generally. This high perception of risk was also found to be the case for governance as a cloud factor. Specifically, the findings show that although there is a perception of a risk in relation to cloud factors, where the sub cloud factors are presented then the respondents often have different ideas, this was the case for governance.

7.3.2.1 Negotiation

There was a correlation between risk and negotiation for governance, however, only three out of the sub cloud factors of governance showed a correlation, they included - the need to have *knowledge and control over data and processes, Assurance about other cloud tenants* and *Knowledge and control over third party issues*. This means that for these areas the perception of risk related to the ability to negotiate. For example, where there was a risk perceived for the need to have *knowledge and control over processes and data,* there is also an associated perceived lack of ability to negotiate. This perceived lack of ability to negotiate was also evident in the interviews.

For compliance and all of the sub cloud factors of compliance, except one there was a correlation between risk and negotiation. Therefore, compliance is a cloud factor where a perception of risk is associated with a lack of ability to negotiate, this was also the case for all of the sub cloud factors of compliance except for compliance when migrating.

Although there was no correlation between risk and negotiation for security and privacy generally, there were correlations for four of the seven sub cloud factors. This would support the idea that there is more insight from government where they are asked in detail about sub cloud factors.

7.3.2.2 Collaboration

Overall there was a very weak link between risk and collaboration. Also, for the effective communication aspect of collaboration, no correlation was found with risk, and for the ability to collaborate effectively there was a weak correlation. This weak correlation was found in relation to governance and compliance.

7.3.2.3 Reputation

A weak correlation was found between risk and reputation generally. It would be expected that there would be a link between risk and reputation, but in this study little correlation was found. Again, as with risk and collaboration the only time that there was a correlation, in this case moderate, was where risk was analysed against reputation in relation to governance and compliance.

Overall, therefore, risk was not a significant factor in terms of its impact on other cloud factors, however, risk cannot be discounted as a factor for reluctance to adopt the public cloud because as a factor in isolation there were perceptions of risk.

7.3.3 Negotiation and Collaboration

There were mixed results in relation to the correlation between negotiation and collaboration as relationship factors. It may be expected that the two are closely correlated because they both involve an active relationship with the CSP. It is important to note that negotiation is pre-signing of the SLA, and collaboration is the ongoing relationship after agreements have been signed. For governance, there was a strong correlation, which means that the government's perceived ability to negotiate has a strong bearing on the perceived ability to collaborate for governance. For compliance and security and privacy there were moderate correlations. This means that the CSP has to improve the negotiation process in order to have a better working relationship on an ongoing basis.

7.3.4 Negotiation and reputation

There was a moderate correlation between the ability to negotiate and the reputation that the government had about the CSP. A moderate correlation was found for all of the cloud factors except performance and offering. Having sufficient information about the cloud provider as an aspect of reputation was even less correlated with the ability to negotiate. Therefore, the government did not feel that their ability to negotiate depended on the information that they had about their CSP.

7.3.5 Collaboration and reputation

Generally, there was very little correlation between the perceived ability to collaborate and the perceived reputation of the CSP. However, if reference to the cloud factors, there was a strong correlation between the perception of a positive reputation and the perceived ability to collaborate for compliance.

7.3.6 Summary

Revealing how relationship factors affect other relationship factors offered a deeper insight into the relationship between government and the CSP. Moreover, the study not only considered the correlations between relationship factors, but also highlights the areas of the cloud where these correlations are significant. The relationship between relationship factors was moderated by the cloud and sub cloud factors, this was evidenced by the fact that a negative perception of one relationship factor for a sub cloud factor was correlated with a negative perception in another relationship factor, and vice versa.

An interesting finding of this study is that where respondents are asked to consider how they feel, as relationship factors, about certain cloud factors, they have more certainty in their opinions. This was found to be true, for example, where respondents were asked if they trusted their CSP generally, they said that they did, but where they were asked about trust in regard to cloud factors they gave either strongly negative or strongly positive answers. This idea was also found to be true in the correlations between the relationship factors, because more significant correlations were found between relationship factors where cloud factors and sub cloud factors were considered.

Trust was found to have not much of an effect on other relationship factors, this was found to be the case for governance, for security and privacy, for performance and offering and most of the relationship factors for compliance. This means that no matter what area of the cloud is being considered by the government, their trust or lack of trust had no bearing on other relationship factors.

One of the problems of collaboration is that the administrative structures are decentralised and there is a need for a central function for organising and distributing information, communication and reminding each partner about the rules that govern the partnership (Thomson et al. 2009). Again, collaboration in this case would be necessary for governments to achieve the cloud critical success factors on an ongoing basis.

7.4 Particular Concern for Government

A study that seeks to determine relationship and cloud factors that may influence the adoption of the public cloud, needs to consider the particular concerns of government. These government-specific concerns were identified in the literature (Ahmad and Janczewski 2011, ENISA, 2011, Diez and Silva, 2013) and are well-known concerns. The results of this study have confirmed these concerns as cloud factors and how they are related to the relationship factors.

Some of the sub cloud factors that are a particular concern of government can be grouped within the same categories, even though they are sub cloud factors of different cloud factors. For example, the results showed that there was a high level of concern for parties other than the CSP themselves, this was evident by the fact that there were high levels of concern about other tenants in the cloud and third parties in addition to the CSP employees themselves. These sub cloud factors were found to be a concern in security and privacy and governance.

Concerns about these sub cloud factors that were confirmed to be a particular concern for government featured in the relationship between relationship factors. Although, for example, insignificant correlations were found between trust and collaboration, there were significant correlation between these relationship factors for sub cloud factors that are of particular concern and relevance to government. For example, there were significant correlations between trust and collaboration for a dynamic SLA and additional specialised staff for government needs. A lack of trust was associated with a lack of confidence to collaborate but mostly in areas that were of particular concern to government, this means that these sub cloud factors had a mediating effect between these relationship factors. Therefore, the sub cloud factors that are government-specific concerns have an impact on the relationship resulting in reluctance to adopt the public cloud.

There was also a high level of concern that the government feel that they cannot get government-specific services, these included dynamic SLAs, tailored security and privacy policy, customisable cloud environment and additional specialised staff for government needs. These are sub cloud factors that are found within the cloud factors.

In order for government to achieve what they need in terms of governance, compliance, security and privacy and performance and offering, they need their specific needs met in each of these areas. The findings in this study, therefore, confirm the idea that was put forward by

DiModica (2014) who said that standardised service can be a problem because it does not allow for differentiated services, something that government require.

These concerns were also echoed in the interviews where it showed that although there was some level of confidence in terms of the relationship factors generally, concerns were expressed about the CSP's ability to meet government specific needs. In fact, the CSP's ability to service the specific needs of government was a condition on the relationship factors, whereby, for example, trust was on condition of security and privacy requirements being met.

The cloud factors that can negatively impact the decision to adopt the cloud, are often categorised within, security and privacy, governance over data and systems, compliance with laws and regulations both domestic and foreign, and the performance of the service as well as contractual conditions. It is accepted by this study that all of these are universal concerns. However, within each of these factors, which are termed as cloud factors in this study, there are sub cloud factors, and some of these, while being a concern for all types of organisation, can also be considered a particular concern for government. There are two reason for this, firstly, the literature has shown that governments have more reasons than other organisations to be concerned about certain issues in the cloud, for example they may require a more flexible SLA or more stringent compliance requirements (Alhamad et al., 2010, Alruwaili and Gulliver, 2014) and secondly, this has been shown in the results of the present study. This also means that the present study had affirmed the concerns that are reflected in the literature.

However, the present study contributes further because not only does it confirm that there are concerns in these cloud areas and that these are impediments to adoption of the public cloud by government, but it goes further to understanding the role of the relationship factors. Where other studies may suggest there is a lack of trust or perception of risk, this study firstly shows specifically, which aspects of the cloud these trust and risk perceptions are, and secondly, extends from merely trust and risk by identifying and incorporating other relationship factors that may have an impact, for example the perceived ability to negotiate or a negative perception of reputation.

A significant finding of this study is that for relationship factors, there was a high level of doubt and lack of confidence in many of the sub cloud factors that are particular to government. Towards the development of the research design of this study, it was important to identify not only the sub cloud factors that would be a concern for any organisation, but

also sub cloud factors that would be a particular concern for government when considering the public cloud.

This idea of the government having negative opinions about sub cloud factors that are a particular concern for government is also supported by the results from the interview. One of the main ideas that arose was that government were very much dependent on the SLA and the SLA contains provisions that directly reflect those sub cloud factors for which there was more confidence, examples include sufficient notice of disruption, migration to the cloud and factors associated with monitoring and auditing activities.

7.5 Recommendations for Cloud Service Provider (CSP)

It would be important for CSPs to take note of the fact that there were some cloud and sub cloud factors where there were significant correlations between different relationship factors. For example, trust in compliance was strongly correlated with the ability to effectively collaborate for compliance and perception of a strong reputation for compliance. Therefore, it is within these particular aspects of the cloud that CSPs should understand these correlations, this, for example, will inform them that they have to improve their collaboration on compliance in order to increase trust of the government, or they have to achieve a positive reputation in compliance in order to achieve trust in compliance. Specifically, this has been found to be true for numerous cloud and sub cloud factors for correlation between relationship factors.

One of the main issues that was identified in the relationship was that there were often concerns about a standardised offering from the CSP. The issue of standardised contracts needs serious reconsideration by the CSP because it is related to many of the concerns that the government have about the cloud which include not being confident about a dynamic SLA, tailored security and privacy policy, a customisable cloud environment, government specific requirements being met and specialised staff for government needs.

Due to the standardised nature of negotiated agreements in the public cloud, roles and responsibilities are often not clear. It is therefore recommended that the CSP address the issue, not only of standardised service agreements, but also create more clarity for roles and responsibilities, which has been perceived negatively by the government.

The results showed that there was an almost complete lack of trust, a perception of risk and a perceived inability to work with the CSP over the security and privacy sub cloud factor of *Assurance regarding CSP employees.* This concern has also been identified in the literature (Venkatraman, 2014, Jansen and Grance, 2011) where proposed solutions include employee background checks and controlled and limited access to servers. Not only does this have to be ensured by the CSP, but the CSP must liaise with the government to find out what standards and level of checks need to be carried and the acceptable level of access to systems.

Overall, although standardisation of the cloud is for economic reasons on the part of the CSP, they have to consider a more tailored solution to attract business from government. The government as a customer will bring large revenues and therefore, there is justification in offering public cloud solution that are not standard.

Trust about governance was found to be a particular issue for government. It is important for the CSP to understand that in order to achieve trust the CSP should not interfere with the clients' applications in the cloud (Abbadi and Alawneh, 2012).

The results of this study showed that the CSPs really need to acknowledge the concerns that government have about governance. Not only were the government concerned about governance generally, but also about the sub cloud factors of governance, especially, there are trust and risk issues related to other tenants, third parties, a dynamic SLA and CSP employees. Therefore, there is a need for the CSP to address these areas. Although the first issue that may come to mind when considering governance is control over data, this was much less of a concern for government than the other areas of governance.

Towards improving collaboration and ensuring trust, the CSP should open their operations to government personnel. A proposed solution is to have cross-organisational teams whereby government employees work with the CSP within their organisation. This would not only allow the CSP to better understand the needs of government, but will also allow government the opportunity for greater governance.

Although overall there was not much significant concern about compliance, it is important for the CSP to understand that they must examine the individual sub cloud factors of compliance towards improving the relationship. For example, the government were not concerned about jurisdiction for the data, however, they were concerned about the location of the data. Therefore, this shows the CSP that they should not make assumptions, government not being

concerned about jurisdiction does not necessarily mean they are not concerned about the location of their data. This principle can be applied to all areas of the cloud.

There was a noticeable perception revealed in the study that the government were very capable of specifying their cloud requirements as part of the ability to negotiate, however, at the same time government perceived that the CSP do not understand these requirements. Therefore, the CSP need to listen and show they are listening and engage a strategy of verification of understanding with the government. Specifically, this could include a mechanism where requests are verified with the CSP for clarity of understanding. This will have repercussions for other relationship factors, for example, it will also increase trust, decrease the perception of risk and improve negotiation and collaboration.

In reference to reputation, the study has shown that a poor reputation is often perceived for the sub cloud factors that are a particular concern for government, for example, CSP employees, third parties and other cloud tenants, but also for compliance generally. It is recommended that the government implement all aforementioned recommendations, which will involve alleviating the government specific concerns, in order improve their reputation in these areas. A specific example that illustrates this idea is that there were positive correlations between trust and reputation for the following sub cloud factors of performance and offering: *Customisable cloud environment, Dynamic / flexible SLA, Meet government specific requirements* and *Additional specialised staff for government needs,* which would inform the CSP that they need to improve their reputation in these areas, possibly through offering them to government as they are not fully provisioned, in order to increase trust.

Finally, the results of the interviews showed that the government had a lack of understanding of the public cloud and that they felt that the public cloud was not suitable for government use. For both of these concerns it is up to the CSP to ensure that the government understand the public cloud and its benefits. This point can also be extended to knowledge about the CSP themselves because the interviews also revealed that the government lacked knowledge about the CSP. By informing the government about the CSP and the public cloud this should alleviate concerns that government have towards increased confidence.

8 Conclusion

Objectives

- **Conclude the implications and contributions of the study**
- **Recommendations for future study**
- **Present limitations**

8.1 Summary of the Thesis

Primarily this study was motivated by the fact that firstly, there is a real need to understand the reasons for the government of Saudi Arabia's reluctance to adopt the public cloud, secondly, the real benefits that the public cloud can bring to the government, and thirdly, the fact that current studies offer a limited understanding through a narrow scope of the relationship between CSP and government as a customer, whereby relationship, organisational or technological factors are considered in isolation. Moreover, the study has shown in the review of the literature not only the benefits of the government adopting the public cloud, but also that it will become necessary in a world where there are increasing threats to countries from terrorism, cyber terrorism and conflict. Therefore, it is imperative that governments move towards a model whereby they can serve their citizens by e-government which can be hosted in a public cloud. While this is the future direction for government in the cloud, it is understandable that governments will have concerns and that some of those concerns will be particular and relevant to government, and it was the aim of this study to understand those concerns through understanding what they are and how they are affected by the relationship between government and CSP.

The study has taken consideration of the relationship between government and CSP to a new level, in that it offers a comprehensive and useful way of examining the relationship. The study has shown that other studies that try to determine the reasons for reluctance to adopt the cloud, especially the public cloud, have a narrow view in that they only consider cloud factors or relationship factors in isolation. Or where studies do consider both, the connection is weak and there is no explicit consideration of the connection and interplay between the two. In this sense, this study has built on these studies, emphasising the relationship while at the same time emphasising the need to consider the detailed aspects of cloud factors.

For both parties, it is important that the concerns are addressed because it is inevitable that government in Saudi Arabia will eventually reside in the cloud. Moreover, concerns that the government in Saudi Arabia have, have to be addressed in a comprehensive way and overcome because of the threats that they face today. Saudi Arabia is a main target of terrorism and that includes cyber terrorism, and although the public cloud is seen by government as something that is vulnerable, the public cloud is also the means to further protect a government in the cloud which has been demonstrated in the case of Estonia. This

study should give more confidence to both parties to move to the public cloud through improving the relationship between them.

In light of such issues, the study set out to further understand in more detail government concerns in Saudi Arabia about adopting the public cloud through understanding relationship and cloud concerns within the context of the relationship. In pursuit of this, the study established aims which were to reveal opinions about relationship and associated cloud factors in the government – Cloud Service Provider (CSP) relationship and to determine specific areas that includes relationship and associated cloud related factors that may have an effect on government confidence in the public cloud. Through the use of questionnaires and interviews this was achieved revealing a deep insight into the concerns that government have about the cloud and the associated relationship factors. Specifically, the association between relationship factors such as trust and cloud factors such as governance was identified in order to further understand the issues within the relationship context, for example, there is a lack of trust in the CSP for governance. This was also achieved through understanding the interplay between two relationship factors and their effect on a cloud factor, for example, a low perception of risk for governance was associated with a perceived ability to negotiate for governance requirements. Therefore, through these approaches the specific areas of concern within the government - CSP relationship were determined.

In reference to the objectives of the study, specific relationship and cloud factors in the government - CSP relationship were thoroughly identified and analysed, through this analysis the second objective, which was to reveal the links between the relationship factors and cloud factors, was also achieved. Overall, the relationship and associated cloud factors as factors that affect the decision to adopt the public cloud were identified through the objective to develop and apply a research method that combines these relationship and cloud factors. Finally, the discussion chapter offered recommendations to CSPs on how the government-CSP relationship can be improved towards increasing government confidence in the public cloud, which was the final objective of the study.

8.2 Contributions

The most apparent contribution of this study has been a new approach to understanding the reasons for reluctance of the Saudi government to use the public cloud for sensitive data and critical systems. This approach has acknowledged that the relationship between government

and the CSP is complex, in that it involves concerns about cloud related technical factors and the relationship factors which should not be considered in isolation, as is the case with other studies. Not only are these two types of factors considered, but the study has also recognised the interplay between the two and the importance of understanding this interplay in understanding the relationship both comprehensively and in detail. The results of the study have further shown that there has been a need to investigate the relationship in this way. Therefore, this study has answered the limitations of other studies (Bhatt, 2012, Aziz et al., 2013, Ahmad and Janczewski, 2011, Lecklider 2014; Wang and Wu 2014, Filali and Yagoubi, 2015, Hana 2013, Alshomrani and Qamar 2013, Almorsy 2011, Fan et al. 2014, Ding et al. 2014) which look at cloud factors in isolation or fail to understand in detail the relationship factors and their association with cloud factors. Issues of trust and risk are well known in the cloud, but specifically, which aspects of the cloud and the context of the relationship are not fully considered or understood.

The study offers a more comprehensive understanding of the relationship between the cloud provider and the government, through understanding how both the relationship factors and the associated cloud factors play a role in that relationship. Moreover, using the research design of the study allowed the relationship factors and the cloud factors to be considered together in order to understand the connections between them, rather than to be considered in isolation. This research design is validated by the fact that the relationship and cloud factors are derived from numerous studies and literature that consider the different factors that may determine the decision to adopt the cloud, this was established in the research design in Chapter 3.

The study has also shown that it is important for both CSPs and government to not just consider the general issues of, for example, security and privacy, or performance and offering, within the relationship but also the detailed aspects of these areas. The study has shown that where more detailed aspects about the cloud are considered it reveals a completely different opinion. This was evidenced by the fact that opinions were often opposed between the general cloud factor such as security and privacy and an associated sub cloud factor such as security related to CSP employees. Moreover, the importance of considering the more detailed aspects of cloud factors through the consideration of sub cloud factors is further proved by the additional levels of concern or negativity where sub cloud factors were considered. This was evident in relation to the relationship factors, whereby, for example, a positive perception of trust in security and privacy soon becomes a negative

perception of trust where sub cloud factors of security and privacy are considered. Therefore, the study informs CSPs of specifically how and where they need to be concerned and how these concerns can be resolved through consideration of both relationship and cloud and sub cloud factors. What has been revealed about the relationship factors is not only important for the CSP and how they deal with the government, but how the government deal with the CSP as well towards achieving increasing government confidence to adopt the public cloud.

Therefore, it was another contribution of the study that recommendations were offered for CSPs on how they can have a better relationship with the government which would include how they could alleviate some of the concerns that government have. Because the research approach revealed a detailed picture of the concerns that government have, it was possible to offer informative and detailed recommendations to the CSP. Specifically, the CSP would, for example, know in which areas of the cloud they are not trusted, or are seen as not being able to understand requirements.

These contributions can be summarised in the following:

1. A new approach to considering the relationship between the government and CSP that includes all relevant relationship and cloud factors together.

2. The development of research design that is designed to reveal relationship and cloud factors in the relationship context and the associations between them.

3. The development of a questionnaire that can be applied to different government-CSP relationship contexts.

4. A deeper insight and understanding of issues in the government-CSP relationship and the reluctance to adopt the public cloud.

5. Recommendations on how to improve the government-CSP relationship towards increasing government confidence in the public cloud.

8.3 Success Criteria Revisited

The first success criterion was to identify the relationship and cloud related issues in the government-CSP relationship. This was achieved successfully through a careful analysis of

the literature including cloud models where the relevant relationship and cloud factors of the government-CSP relationship were identified. The second success criterion which was to identify the associations between relationship and cloud factors was achieved through the application of the questionnaire and the analysis of the results. The research design was successfully developed and applied through the use of the questionnaire, this was the third criterion. For the fourth criterion, the potential issues that may affect cloud adoption were identified in the questionnaire and the interview results and these issues were used in the successful development of recommendations for CSPs which was the fifth criterion of the study.

8.4 Implications

The study has implications for the various stakeholders that are involved in the government – CSP relationship. Importantly, the study has implications for CSPs who are seeking to have government use the public cloud, this is because the study highlights in detail the reasons that government may be reluctant to adopt the public cloud. These reasons may be associated with relationship factors in which case the cloud provider could adjust their behaviour or how they deal with the government as a customer, or could be associated with cloud factors in which case the government could change services to alleviate these concerns, or the reasons could be associated with the links between relationship and cloud factors. In reference to the latter point, this study would allow CSPs to go beyond simply enhancing their services as a solution to government reluctance, instead they could, for example, alleviate the perception of the inability to negotiate certain cloud factors, or improve their reputation for certain cloud factors. As it has been stated in the study, to understand the cloud factors where there are concerns is not enough, and to understand the relationship issues in isolation also has its limitations. It is not enough for a CSP to know that they are not trusted, they need to understand which aspect of the cloud are they not trusted in, likewise it is not enough to know that a potential customer has concerns about security, the CSP needs to know how to address that concern, for example do they have to alleviate perception of risk or to understand the customers' needs better.

The study also has implications for the government organisations in Saudi Arabia that are responsible for decision making for the adoption of the public cloud. Where the cloud is adopted it will not be used by one agency within the government, instead there will be

numerous agencies on numerous levels, involving numerous employees, so the government decision maker can understand the potential concerns of users, or at least understand the areas that need to be addressed.

For the research and academic fields the study has implications for how the relationship between government and CSP plays a role in decision making to adopt the cloud. In addition to studies that offer consideration of organisational factors, this study offers a new research design based on relationship and cloud factors. Moreover, there is the possibility that the principles of this research design can be applied in other IT and IS procurement situations, for government or otherwise.

8.5 Limitations

There was an intensive investigation into the cloud factors to the extent that the study included sub cloud factors. However, although for some of the relationship factors, such as negotiation, more detailed aspects were considered, this was not applied to all the relationship factors. A future study could consider more of the aspects of the relationship factors, for example the different dimensions of trust could be considered.

The study was set in Saudi Arabia and it is reasonable to expect that cultural beliefs may have an impact on the relationship with the CSP. The study focused on the relationship but there was no consideration of how cultural factors would influence this relationship. Some CSPs are local, and some, especially those that offer the public cloud, are international and issues of trust and risk could be affected by cultural differences.

8.6 Future study

One of the findings of the present study was that the government felt that they could not negotiate or collaborate with the CSP on sub cloud factors that were a particular concern or relevance to government. While the present study offered detail on the specific sub cloud factors where this lack of confidence to negotiate and collaborate was found, it did not address the reasons for the inability to negotiate and collaborate. Towards offering those who provide public cloud services to government a better understanding of their client, a future study could further investigate the reasons why there is a perceived inability in these areas. The inability could be a fault of the CSP which could mean that they lack the ability to

negotiate or collaborate, or it could be perception of the CSP's inability to offer the service that the government require.

This study offered a research design to further understand the relationship and the reluctance by government to adopt the public cloud. A future study can look at the possibility of taking the concept of the approach by this study and develop a model or framework that can be used by both cloud customer and cloud provider alike, to be applied to a specific situation to further guide how the relationship should be approached. The main objective of such a future study would consider how the features of the research design of this study can be translated to a model that can be applied practically.

The present study was concerned with a specific context. A future study could look at the feasibility of using the research design work in other contexts. For example, the study, or indeed any derived applicable models, as mentioned in the above, could be applied in different contexts with different types of organisation. This could reveal the particular concerns of different types of organisation, as this study has revealed particular concerns of the government of Saudi Arabia.

One of the findings of the study was that where respondents were questioned about cloud factors generally, there was less concern, and where questioned about more detailed aspects of these cloud factors, namely, the sub cloud factors, there was more concern in many cases. This showed an apparent contradiction in the responses, for example, on the issue of security and privacy generally, there was a high level of trust but for some of the sub cloud factors of security and privacy there was a low level of trust. Therefore, a future study could investigate further this phenomenon and look at why there are perceived differences between cloud factors and associated sub cloud factors. For example, are the responses to the sub cloud factors a result of having much or little knowledge for that particular factor? Moreover, a future study could investigate the implications that these results would have for decision making and understanding cloud-related concerns, as opposed to other studies that simply address the cloud factors.

In reference to one of the limitations of the study, a future study could investigate the relationship using more detailed aspects of relationship factors. Although relevant aspects of the relationship factors in a government-CSP relationship were considered, a future study could identify and apply more aspects of these relationship factors towards understanding government reluctance to adopt the public cloud.

A more focused study could be conducted which investigates the link between relationship and associated cloud factors and the confidence to adopt the cloud, in other words what is the causal link between the identified factors and the confidence or otherwise to adopt the public cloud?

References

Aamir, M. Hong, X. Ali, A., Tahir, M., Asif, M. (2014). Cloud Computing security challenges and their compromised attributes.. *International Journal of Scientific Engineering and Technology,* 3 (4), pp. 395-399.

Abbadi, I.M. and Alawneh, M., (2012). A framework for establishing trust in the cloud. *Computers & Electrical Engineering*, 38 (5), pp. 1073-1087.

Ahmad, M. and Hasibuan, Z.A., (2012). Government services integration based on cloud technology. *In Proceedings of the 14th International Conference on Information Integration and Web-based Applications & Services*, pp. 303-306. ACM.

Ahmad, R. and Janczewski, L., (2011). Governance life cycle framework for managing security in public cloud: from user perspective. In *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, pp. 372-379.

Ahmed, M. and Hossain, M.A., (2014). Cloud computing and security issues in the cloud. *International Journal of Network Security & Its Applications*, 6 (1), pp. 25-36.

Alam, B., Doja, M.N., Alam, M. and Malhotra, S., (2013). Security Issues Analysis for cloud computing. *International Journal of Computer Science and Information Security*, 11 (9), p. 117.

Alghanim, W. and Chen, F. (2016). A Relationship Approach to Increasing Government Confidence in the Public Cloud for Sensitive Data Deployment. *International Journal of Research in Science and Technology*. 6 (III), pp. 25-36.

Alghanim, W. and Chen, F. (2016). Building Public Confidence in the Public Cloud through Improved SLAs. *International Journal of Research in Science and Technology*. 6 (III), pp. 37-43.

Alghanim, W. and Chen, F. (2016). Suitability of Frameworks, Standards and Certification For Government Adoption of the Public Cloud For Advance Digital Continuity. *International Journal of Research in Science and Technology*. 6 (III), pp. 14-24.

Alghanim, W. and Chen, F. (2017). Relationship And Cloud Factors Affecting Government Confidence In The Public Cloud. *International Journal Of Research In Science & Technology*. 7 (1), pp. 1-8.

Alhamad, M., Dillon, T. and Chang, E., (2010). Sla-based trust model for cloud computing. In *Network-Based Information Systems (NBiS), 2010 13th International Conference on* pp. 321-324.

Alharbi, S.T., (2012). Users' acceptance of cloud computing in Saudi Arabia: an extension of technology acceptance model. *International Journal of Cloud Applications and Computing (IJCAC), 2* (2), pp.1-11.

Alkhater, N., Wills, G. and Walters, R., (2014). Factors influencing an organisation's intention to adopt cloud computing in Saudi Arabia. *In Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on,* pp. 1040-1044.

Almorsy, M. Grundy, J. Ibrahim, A., (2011). Collaboration-Based Cloud Computing Security Management Framework. *2011 IEEE 4th International Conference on Cloud Computing*. 1 (1), pp. 364 - 371.

Alruwaili, F.F. and Gulliver, T. A., (2014). Trusted CCIPS: A Trust Security Model for Cloud Services Based on a Collaborative Intrusion Detection and Prevention Framework. *International Journal of Latest Trends in Computing*, 5 (1).

Alshomrani, S. and Qamar, S., (2013). Cloud based e-government: benefits and challenges. *International Journal of Multidisciplinary Sciences and Engineering, 4* (6), pp. 1-7.

Andreeva, A. (2014). *Cloud Storage Security: AWS Vs. Azure.*Available: http://www.networkcomputing.com/cloud-infrastructure/cloud-storage-security-aws-vs-azure/a/d-id/1306605. Last accessed 6th August, 2015.

Anitha, Y. (2013). Security Issues in Cloud Computing - A Review. *International Journal of Thesis Projects and Dissertations*. 1 (1), pp. 1 - 6.

Anthes, G. (2015). Estonia: A Model for e-Government. *Communications Of The ACM*. 58 (6), 18 - 20.

Australian Government. (2011). Community Cloud Governance – An Australian Government perspective.Available https://www.finance.gov.au/sites/default/files/community_cloud_governance_better_practice_guide.pdf. Last accessed 6th August, 2014.

Aziz, M. Abawajy, J. Chowdhury, M. (2013). The Challenges of Cloud Technology Adoption in E-Government. *International Conference on Advanced Computer Science Applications and Technologies*, pp. 470 - 473.

Bamiah, M., Brohi, S., Chuprat, S. and Brohi, M.N., (2012). Cloud implementation security challenges. In *Cloud Computing Technologies, Applications and Management (ICCCTAM), International Conference on*, pp. 174-178.

Barkin, R., (2013). Finding The Perfect Match, *Penton Media, Inc., Penton Business Media, Inc*, Pittsfield.

Baset, S.A., (2012). Cloud SLAs: present and future. *ACM SIGOPS Operating Systems Review,* 46 (2), pp. 57-66.

Bhardwaj, S., Jain, L. and Jain, S., (2010). Cloud computing: A study of infrastructure as a service (IAAS). *International Journal of engineering and information Technology*, 2 (1), pp. 60-63.

Bhatt, D., (2011). A Revolution In Information Technology-Cloud Computing. *Walailak Journal of Science and Technology* (WJST), 9 (2), pp. 107-113.

Blomqvist, K., (2002). Partnering in the dynamic environment: The role of trust in asymmetric technology partnership formation. *Lappeenranta University of Technology*.

Blomqvist, K., Hurmelinna-Laukkanen, P., Nummela, N. and Saarenketo, S., (2008). The role of trust and contracts in the internationalization of technology-intensive Born Globals. *Journal of Engineering and Technology Management*, *25* (1), pp. 123-135.

Blomqvist, K., Hurmelinna, P. and Seppänen, R., (2005). Playing the collaboration game right—balancing trust and contracting. *Technovation*, *25* (5), pp. 497-504.

Bo, L., (2013). Study on massive e-government data cloud storage scheme based on Hadoop. *In Software Engineering and Service Science (ICSESS), 4th IEEE International Conference on*, pp. 434-437.

Borgman, H.P., Bahli, B., Heier, H. and Schewski, F., (2013). Cloudrise: exploring cloud computing adoption and governance with the TOE framework. *In System Sciences (HICSS), 46th Hawaii International Conference on*, pp. 4425-4435.

Brace, I., (2008). Questionnaire design: How to plan, structure and write survey material for effective market research. *Kogan Page Publishers*.

Brender, N. and Markov, I., (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International journal of information management*, 33 (5), pp. 726-733.

Brohi, S.N. and Bamiah, M.A., (2011). "Challenges and Benefits for Adoption the Paradigm of Cloud Computing", *International Journal of Advanced Engineering Sciences and Technology*, 8 (2), pp. 286-290.

Burda, D. and Teuteberg, F., (2014). The role of trust and risk perceptions in cloud archiving—Results from an empirical study. *The Journal of High Technology Management Research*, *25* (2), pp. 172-187.

Cahoy, E., (2015). Empirical Research in Education and the Behavioral/Social Sciences. Available: http://psu.libguides.com/emp. Last accessed 21st November, 2015.

Chanchary, F.H. and Islam, S., (2011). E-government based on cloud computing with rational inference agent. In *High Capacity Optical Networks and Enabling Technologies (HONET)*, pp. 261-266.

Chandra, D.G. and Bhadoria, R.S., (2012). Cloud computing model for National E-governance Plan (NeGP). *In Computational Intelligence and Communication Networks (CICN), Fourth International Conference on*, pp. 520-524.

Cloud Security Alliance., (2011). Security Guidance for Critical Areas of Focus in Cloud Computing v.3.0. CSA, pp 1 - 162.

Cohen, L., Manion, L. and Morrison, K., (2013). Research methods in education. *Routledge*.

Communications and Information Technology Commission., (2016). Public Consultation Document on the Proposed Regulation for Cloud Computing. CITC. Available:http://www.citc.gov.sa/en/new/publicConsultation/Documents/143703_en.pdf. Last accessed 6th April, 2015.

Craig, R., Frazier, J., Jacknis, N., Murphy, S., Purcell, C., Spencer, P. and Stanley, J., (2009). Cloud computing in the public sector: public manager's guide to evaluating and adopting cloud computing. *White Paper. Cisco Internet Business Solutions Group*.

Creswell, J.W., (2013). Research design: Qualitative, quantitative, and mixed methods approaches. *Sage publications*.

Crossan, F., (2003). Research philosophy: towards an understanding. *Nurse researcher*, *11* (1), pp. 46-55.

Das, R.K., Patnaik, S. and Misro, A.K., (2011). Adoption of cloud computing in e-governance. *Advanced computing*, pp. 161-172.

Dash, N. (2005). Module: Selection of the Research Paradigm and Methodology. Available: http://www.celt.mmu.ac.uk/researchmethods/Modules/Selection_of_methodology/index.php. Last accessed 25th October, 2016.

Dash, N.K., (2005). Module: Selection of the research paradigm and methodology. Retrieved August, 9, p.2009.

De la Prieta, F., Heras, S., Palanca, J., Rodríguez, S., Bajo, J. and Julián, V., (2015). Real-time agreement and fulfilment of SLAs in Cloud Computing environments. *AI Communications*, *28* (3), pp. 403-426.

Dečman, M. and Vintar, M., (2013). A possible solution for digital preservation of e-government: A centralised repository within a cloud computing framework. *In Aslib Proceedings*, 65 (4), pp. 406-424.

Department of Defense., (2012). Department of Defense Information Assurance Certi cation and Accreditation Process (DIACAP). Available: http://www.prim.osd.mil/Documents/DIACAP_Slick_Sheet.pdf.

Di Modica, G. and Tomarchio, O., (2015). Matching the business perspectives of providers and customers in future cloud markets. *Cluster Computing*, *18* (1), pp. 457-475.

Diez, O. and SIlva, A., (2013). Govcloud: Using cloud computing in public organizations. *IEEE technology and society magazine, 32* (1), pp. 66-72.

Ding, S., Yang, S., Zhang, Y., Liang, C. and Xia, C. (2014). Combining QoS prediction and customer satisfaction estimation to solve cloud service trustworthiness evaluation problems. *Knowledge-Based Systems*, 56, pp.216-225.

Doelitzscher, F. Fischer, C. Moskal, D. Reich, C. Knahl, M. Clarke, M., (2012). Validating Cloud Infrastructure Changes By Cloud Audits. *2012 IEEE Eighth World Congress on Services*, 377 - 384.

Doney, P.M. and Cannon, J.P., (1997). An examination of the nature of trust in buyer-seller relationships. *the Journal of Marketing*, pp. 35-51.

Duncan, B. and Whittington, M., (2014). Compliance with standards, assurance and audit: does this equal security?. *In Proceedings of the 7th International Conference on Security of Information and Networks*, p. 77.

Dunne, M., (2014). Isg: Strategies And Tactics For Information Security Governance, Cloud Security Alliance And Government Cloud. *eForensics*. [online] Available at: https://eforensicsmag.com/download/2586/.

Elena, G., (2012). Risk Perception and Cloud Computing Security. *dcs. gla. ac. uk*.

ENISA., (2011). Security & Resilience in Governmental Clouds - Making an informed decision. *ENISA.*, pp. 1 - 141.

ENISA., (2015). Security Framework for Governmental Clouds. *European Union Agency for Network and Information Security*, pp. 1 -34.

European Union Agency for Network and Information Security. (2015). Security Framework for Governmental Clouds. *ENISA*, pp. *1-33*.

Fan, W. and Perros, H., (2014). A novel trust management framework for multi-cloud environments based on trust service providers. *Knowledge-Based Systems, 70*, pp. 392-406.

Fan, W., Yang, S. and Pei, J., (2014). A novel two stage model for cloud service trustworthiness evaluation. *Expert Systems*, 31(2), pp.136-153.

Filali, F.Z. and Yagoubi, B., (2015). Global trust: A trust model for cloud service selection. *International Journal of Computer Network and Information Security, 7* (5), p. 41.

Firdhous, M., Ghazali, O. and Hassan, S., (2012). Trust management in cloud computing: a critical review. *arXiv preprint arXiv:1211.3979*.

Fraley, R.C. and Vazire, S., (2014). The N-pact factor: Evaluating the quality of empirical journals with respect to sample size and statistical power. *PloS one, 9* (10), p.e109019.

Gholami, A. and Arani, M.G., (2015). A trust model based on quality of service in cloud computing environment. *International Journal of Database Theory and Application*, *8* (5), pp. 161-170.

Gillham, B. (2000). The research interview, Continuum, London.

Gillham, B. (2007). Research interviewing: the range of techniques. *Open University Press, Maidenhead.*

Gillham, B. (2008). Developing a questionnaire. *A&C Black.*

Gillham, B., (2005). Research Interviewing: The range of techniques: A practical guide. McGraw-Hill Education (UK).

Goo, J. and Huang, C.D., (2008). Facilitating relational governance through service level agreements in IT outsourcing: An application of the commitment–trust theory. *Decision Support Systems*, *46* (1), pp. 216-232.

Grudinschi, D., Sintonen, S. and Hallikas, J., (2014). Relationship risk perception and determinants of the collaboration fluency of buyer–supplier relationships in public service procurement. *Journal of Purchasing and Supply Management*, *20* (2), pp. 82-91.

Haag, S. and Eckhardt, A., (2014). Organizational cloud service adoption: a scientometric and content-based literature analysis. *Journal of Business Economics*, *84* (3), pp. 407-440.

Haag, S., Eckhardt, A. and Kronung, J., (2014). From the Ground to the Cloud--A Structured Literature Analysis of the Cloud Service Landscape around the Public and Private Sector. *In System Sciences (HICSS), 2014 47th Hawaii International Conference on*, pp. 2127-2136.

Habib, S.M., Hauke, S., Ries, S. and Mühlhäuser, M., (2012). Trust as a facilitator in cloud computing: a survey. *Journal of Cloud Computing: Advances, Systems and Applications*, *1* (1), p. 19.

Habib, S.M., Ries, S. and Muhlhauser, M., (2011). Towards a trust management system for cloud computing. *In Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 10th International Conference on*, pp. 933-939.

Halcomb, E. and Hickman, L., (2015). Mixed methods research. *Nursing Standard*, *29* (32), pp. 41-47.

Hana, M.A., (2013). E-government cloud computing proposed model: Egyptian E_Government Cloud Computing. *In Advances in Computing, Communications and Informatics (ICACCI), International Conference on*, pp. 847-852.

Hashemi, S., (2013). Cloud Computing Technology for Egovernment ARCHITECTURE. *International Journal in Foundations of Computer Science & Technology*, 3 (6), pp. 15 - 23.

Hashizume, K. Rosado, D. Fernandez-Medina, E. Fernandez, E., (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, 4 (5), pp. 1 - 13.

Hoffmann, W.H. and Schlosser, R., (2001). Success factors of strategic alliances in small and medium-sized enterprises—An empirical survey. *Long range planning*, *34* (3), pp. 357-381.

Holloway, I., Wheeler, S, (2010). Qualitative research in nursing and healthcare, 3rd Edition, *Wiley-Blackwell, Oxford.*

Hon, W.K., Millard, C. and Walden, I., (2012). Negotiating cloud contracts: Looking at clouds from both sides now. *Stan. Tech. L. Rev.*, *16*, p. 79.

Howitt, D. and Cramer, D., (2007). Introduction to research methods in psychology, *Pearson Education.*

Howitt, D. and Cramer, D., (2011). Thematic analysis. *Qualitative Research and Educational Sciences: A Reader about Useful Strategies and Tools*, pp. 179-202.

Huang, J. and Nicol, D.M., (2013). Trust mechanisms for cloud computing. *Journal of Cloud Computing: Advances, Systems and Applications*, *2* (1), p. 9.

Huntgeburth, J., (2015). Developing and Evaluating a Cloud Service Relationship Theory. *Springer International Publishing*.

Huntgeburth, J., Förderer, J. and Veit, D.J., (2013). Up in the Cloud: Understanding the Chasm between Expectations and Reality. *Thirty Fourth International Conference on Information Systems, Milan*.

Inouye, J., (2014). Campbell Institute. Risk Perception; Theories, Strategies and Next Steps. National Safety Council. Available: http://www.nsc.org/CambpellInstituteandAwardDocuments/WP-Risk%20Perception.pdf. Last accessed 6th August, 2015.

Jansen, W. and Grance, T., (2011). NIST Sp 800-144. guidelines on security and privacy in public cloud computing.

Johansson, B. and Lahtinen, M., (2012). Requirement specification in government IT procurement. *Procedia Technology*, *5*, pp. 369-377.

Jupp, V. (2006). The SAGE dictionary of social research methods, *Sage Publications*.

Kanwal, A., Masood, R., Shibli, M.A. and Mumtaz, R., (2014). Taxonomy for Trust Models in Cloud Computing. *The Computer Journal*, p.bxu138.

Khan, F., Zhang, B., Khan, S. and Chen, S., (2011). Technological leap frogging e-government through cloud computing. *In Broadband Network and Multimedia Technology (IC-BNMT), 2011 4th IEEE International Conference on*, pp. 201-206.

Khan, K.M. and Malluhi, Q., (2010). Establishing trust in cloud computing. *IT professional*, *12* (5), pp. 20-27.

Kidman, A., (2013). *Top 10 Lesser-Known Facts About Windows Azure Security.* Available: http://www.lifehacker.com.au/2013/04/top-ten-lesser-known-facts-about-windows-azure-security/. Last accessed 6th August, 2015.

King, N. and Horrocks, C., (2010). Interviews in qualitative research. *Sage*.

Koza, M. and Lewin, A., (2000). Managing partnerships and strategic alliances: raising the odds of success. *European Management Journal*, *18* (2), pp. 146-151.

Kurdi, R., Taleb-Bendiab, A., Randles, M. and Taylor, M., (2011). E-government information systems and cloud computing (readiness and analysis). In *Developments in E-systems Engineering (DeSE), 2011*, pp. 404-409.

Kvale, S. Brinkmann, S. (2009) Interviews - Learning the Craft of Qualitative Research Interviewing. *2nd ed. Thousand Oaks: SAGE Publications.*

Kvale, S., (2008). Doing interviews. *Sage*.

Lecklider, T., (2014). Good enough for government work. *EE-Evaluation Engineering*, *53*(12), pp.18-20.

Liang, J., (2012). Government cloud: enhancing efficiency of e-government and providing better public services. In *Service sciences (IJCSS), 2012 international joint conference on*, pp. 261-265.

Luna, J., Ghani, H., Germanus, D. and Suri, N., (2011). A security metrics framework for the cloud. In *Security and Cryptography (SECRYPT), 2011 Proceedings of the International Conference on*, pp. 245-250.

Macías, M. and Guitart, J., (2014). SLA negotiation and enforcement policies for revenue maximization and client classification in cloud providers. *Future Generation Computer Systems*, *41*, pp. 19-31.

Manuel, P., (2015). A trust model of cloud computing based on Quality of Service. *Annals of Operations Research*, *233* (1), pp. 281-292.

Matthews, B. & Ross, L., (2010). Research methods: a practical guide for the social sciences, Longman, Harlow.

Mayer, R.C., Davis, J.H. and Schoorman, F.D., (1995). An integrative model of organizational trust. Academy of management review, *20* (3), pp. 709-734.

McKnight, D.H. and Chervany, N.L., (2001). Conceptualizing trust: A typology and e-commerce customer relationships model. *In System Sciences, 2001. Proceedings of the 34th Annual Hawaii International Conference on*, p. 10.

Merriam, S.B., (2009). Qualitative research: a guide to design and implementation, Rev. edn, *Jossey-Bass*, San Francisco.

Microsoft., (2015). *Microsoft Azure Trust Center*. Available: https://azure.microsoft.com/en-us/support/trust-center/. Last accessed 10th July, 2015.

Ministry of Communications and Information Technology., (2017). Government Cloud Computing. Available:http://www.yesser.gov.sa/en/BuildingBlocks/Pages/GCloud_Computing.aspx. Last accessed 1st February 2017.

Ministry of Economic Affairs and Communications and Microsoft., (2015). Implementation of the Virtual Data Embassy Solution. Available:https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf. Last accessed 1st February 2015.

Mohammed, F. and Ibrahim, O., (2015). Models of adopting cloud computing in the e-government context: a review. *Jurnal Teknologi*, 73 (2), pp. 51-59.

Mreea, M., Munasinghe, K. and Sharma, D., (2016). A strategic decision value model for cloud computing in Saudi Arabia's public sector. *In Computer and Information Science (ICIS), 2016 IEEE/ACIS 15th International Conference on*, pp. 1-7.

Mudge, C. (2010). Cloud Computing: Opportunities and Challenges for Australia, report of a study by the Australian academy of Technological sciences and engineering (ATSE). Available:https://www.atse.org.au/Documents/reports/cloud-computing-opportunities-challenges-australia.pdf. Last accessed 6th May, 2015.

Mudge, C., (2010). CLOUD COMPUTING: opportunities and challenges for australia. *Australian Academy of Technological Sciences and Engineering*.

Mukherjee, K. and Sahoo, G., (2012). A novel methodology for security and privacy of cloud computing and its use in e-Governance. *In Information and Communication Technologies (WICT), 2012 World Congress on*, pp. 561-566.

Nasr, A.A.O., (2012). The application of cloud computing in e-government systems *(Doctoral dissertation, Cairo University).*

Neuman, W.L., (2014). Social research methods: qualitative and quantitative approaches. *Seventh Pearson new international edn, Pearson, Harlow, Essex.*

Noor, T.H. and Sheng, Q.Z., (2011). Credibility-based trust management for services in cloud environments. In *International Conference on Service-Oriented Computing*, pp. 328-343.

Noor, T.H., Sheng, Q.Z., Maamar, Z. and Zeadally, S., (2016). Managing Trust in the Cloud: State of the Art and Research Challenges. *Computer*, *49* (2), pp. 34-45.

Noor, T.H., Sheng, Q.Z., Zeadally, S. and Yu, J., (2013). Trust management of services in cloud environments: Obstacles and solutions. *ACM Computing Surveys (CSUR)*, *46* (1), p. 12.

Nycz, M. and Polkowski, Z., (2015). Cloud Computing in Government Units. In *Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on*, pp. 513-520.

Paquette, S., Jaeger, P.T. and Wilson, S.C., (2010). Identifying the security risks associated with governmental use of cloud computing. *Government information quarterly*, *27* (3), pp. 245-253.

Pilevari, N., Toloei, A. and Sanaei, M., (2013). A model for evaluating cloud-computing users' satisfaction. *African Journal of Business Management*, *7* (16), p. 1405.

Prasad, A., Chaurasia, S., Singh, A. and Gour, D., (2010). Mapping Cloud computing onto useful E-Governance. *arXiv preprint arXiv:1009.2314*.

Rastogi, A., (2010). A model based approach to implement cloud computing in e-Governance. *International Journal of Computer Applications*, *9* (7), pp. 15-18.

Rebollo, O. Mellado, D. Fernández-Medina, E., (2012). A Systematic Review of Information Security Governance Frameworks in the Cloud Computing Environment. *Journal of Universal Computer Science*. 18 (6), 798 - 815.

Rothstein, J.R., (2007). Managing IT Procurement Risks. *EDPAC: The EDP Audit, Control, and Security Newsletter*, *36* (3-4), pp. 13-25.

Ryan, P. and Falvey, S., (2012). Trust in the clouds. *Computer law & security review*, *28* (5), pp. 513-521.

Sarker, S., Chatterjee, S. and Xiao, X., (2013). How "sociotechnical" is our IS research. In *An assessment and possible ways forward," in 2013 Thirty Fourth International Conference on Information Systems, Milan*.

Saunders, M., Lewis, P. & Thornhill, A., (2016). Research methods for business students. 7th Edition, *Pearson Education, Harlow*.

Saunders, M., Lewis, P. & Thornhill, A., (2007). Research methods for business student. *4th edn, Financial Times Prentice Hall, Harlow.*

Scotland., (2014). Scotland's Digital Future: Data Hosting and Data Centre Strategy for the Scottish Public Sector. *Digital Scotland*, pp. 1 - 39.

Seidman, I., (2013). Interviewing as qualitative research: a guide for researchers in education and the social sciences, 4th edn, *Teachers College Press*, New York.

Sharma, M.K. and Thapliyal, M.P., (2011). G-Cloud–(e-Governance in Cloud). *International Journal Engg. TechSci*, *2* (2), pp. 134-137.

Simmonds, P., Yeomans, A., Dobson, I., Arnold, J., Secombe, A., Johnson, P., Tully, S., Ramamorthy, B., Kumaraswamy, S., Mishra, R. and Lang, U., (2011). Security Guidance for Critical Area of Focus in Cloud Computing v3. 0. Cloud Security Alliance (CSA).

Smith, J.A., Breakwell, G.M. & Wright, D.B., (2012). Research methods in psychology, 4th Edition, *SAGE*, London.

Spiga, Daniele, Enrico Fattibene, Matteo Manzali, Davide Salomoni, Valerio Venturi, Paolo Veronesi, Livio Fanò et al. (2014). A Cloud-based solution for Public Administrations. Available:https://www.researchgate.net/profile/Barbara_Re/publication/269272484_A_cloud based_solution_for_public_administrations_The_experience_of_the_Regione_Marche/links/ 551676c20cf2d70ee274aac2.pdf. Last accessed 1st February 2016.

Takabi, H., Joshi, J.B. and Ahn, G.J., (2010). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy*, *8* (6), pp. 24-31.

Tashkandi, A. and Al-Jabri, I., (2015). Cloud Computing Adoption by Higher Education Institutions in Saudi Arabia: Analysis Based on TOE. *In Cloud Computing (ICCC), 2015 International Conference on*, pp. 1-8.

Thomson, A.M., Perry, J.L. and Miller, T.K., (2009). Conceptualizing and measuring collaboration. *Journal of Public Administration Research and Theory*, *19* (1), pp. 23-56.

Tracy, S.J., (2013). Qualitative research methods: collecting evidence, crafting analysis, communicating impact. *Wiley-Blackwell*, Chichester.

Trenz, M., Huntgeburth, J.C. and Veit, D., (2013). June. The Role Of Uncertainty In Cloud Computing Continuance: Antecedents, Mitigators, And Consequences. In *ECIS*, p. 147.

Trigueros-Preciado, S., Pérez-González, D. and Solana-González, P., (2013). Cloud computing in industrial SMEs: identification of the barriers to its adoption and effects of its application. *Electronic Markets*, 23(2), pp.105-114.

Tripathi, A. and Parihar, B., (2011). E-governance challenges and cloud benefits. *In Computer Science and Automation Engineering (CSAE), IEEE International Conference on* (1), pp. 351-354.

Tullis, T. & Albert, B, (2013). Measuring the User Experience: Collecting, Analyzing, and Presenting Usability Metrics, Second; 2nd; edn, *Morgan Kaufmann Publishers Inc, US.*

Venkatraman, A., (2014). *Azure CTO Mark Russinovich's top ten public cloud security risks.* Available: http://www.computerweekly.com/news/2240232396/How-to-mitigate-top-ten-public-cloud-security-risks-Azure-CTO-Mark-Russinovich. Last accessed 6th August, 2015.

Walliman, N,. (2011). Research Methods. Oxon: Routledge.

Wang, L. and Wu, Z., (2014). A Trustworthiness Evaluation Framework in Cloud Computing for Service Selection. *In Cloud Computing Technology and Science (CloudCom), IEEE 6th International Conference on*, pp. 101-106. IEEE.

Wang, P. and Hua, H., (2011). A model of government information value-added exploitation based on cloud computing. In *Business Management and Electronic Information (BMEI), 2011 International Conference on* (2), pp. 518-522. IEEE.

Wiseman, R.M., Cuevas‐Rodríguez, G. and Gomez‐Mejia, L.R., (2012). Towards a social theory of agency. *Journal of Management Studies*, *49* (1), pp. 202-222.

Wu, C. and Marotta, S., (2013). Framework for Assessing Cloud Trustworthiness. In *Cloud Computing (CLOUD), 2013 IEEE Sixth International Conference on*, pp. 956-957.

Wu, L., Garg, S.K. and Buyya, R., (2012). SLA-based admission control for a Software-as-a-Service provider in Cloud computing environments. *Journal of Computer and System Sciences*, *78*(5), pp. 1280-1299.

Xiao, X., (2013). How" Sociotechnical" is our IS Research?: An Assessment and Possible Ways Forward. In *The 34th International Conference on Information Systems. ICIS 2013*.

Yamin, M., (2013). Cloud economy of developing countries. *World*, *3*(3).

Zwattendorfer, B. and Tauber, A., (2013). The public cloud for e-government. *International Journal of Distributed Systems and Technologies (IJDST)*, *4* (4), pp. 1-14.

Zwattendorfer, B., Stranacher, K., Tauber, A. and Reichstädter, P., (2013). Cloud computing in e-government across europe. *In International Conference on Electronic Government and the Information Systems Perspective*, pp. 181-195.

APPENDIX

Confidence of Government in the Public Cloud

Participant Information Sheet (Questionnaire)

Dear Senior,

We would like you to take part in a study about conducted by a researcher at De Montfort University in the United Kingdom.

Introduction to the study

Increasingly governments are using cloud technology to host data and services. However, there is reluctance to place sensitive data in public clouds because of security and privacy concerns. These concerns are related to governance in the public cloud and compliance with laws. When sensitive data is stored in a public cloud, governments lose a certain amount of control. Although there is willingness by governments to use the public cloud for sensitive data, unless above issues are resolved, advancement in this area will be slow. Through critical analysis of existing standards, this study proposes a new approach to the governance of the government-cloud provider relationship towards increasing confidence in placing sensitive data in the public cloud.

Participation in this study is voluntary and will involve a questionnaire, which will take approximately 10 to 15 minutes.

Participation is voluntary and you have the right to withdraw at any point during the research. Upon withdrawal from the research all of the obtained identifiable data will be destroyed, however, once the data has been anonymised it cannot be destroyed because it will be impossible to identify the origin of the data.

Excerpts from the questionnaires will be used in any publications derived from this study.

Confidentiality, privacy and anonymity are assured. If the researcher wants to use any quotations it will be anonymous. The distribution of the questionnaire will be through an online survey system, which will mean there is no identifying information, you will simply click on a link, complete the questionnaire and submit it.

The information that is gained in this research project will not be used for another project and will only be used strictly for purposes highlighted above.

All data will be kept in a secure location and is only accessible to the researcher and you will be able to request data at any time.

إذا تفضل الحصول على نسخة باللغة العربية الرجاء الاتصال بالباحث

If there are any questions regarding this research please contact: http://soo.gd/Questionnaire

Waleed Al Ghanim (PhD Researcher)

Faculty of Technology, *De Montfort University*, 49 Oxford Street, Innovation Centre, LE1 5XY, Leicester, UK

P10003240@myemail.dmu.ac.uk TEL: +44 7593042025

Confidence of Government in the Public Cloud

Consent form for questionnaire - Senior

Issue	Participant's initial
I have read the information provide in the information sheet about the study titled " Confidence of Government in the Public Cloud".	
I have been given the opportunity to ask questions about this study, the answers were satisfactory and I was provided with additional information that I requested.	
I understand that participation is voluntary and I have the right to withdraw from the study at any time and my data destroyed.	
I am aware of the fact that excerpts from the questionnaire may be used in publications derived from this study, and all data will be anonymised.	
I have been informed that the data will be kept secure and will be for research purposes only and at any time I can request a copy of the data or remove my data. I have also been made aware that the survey will be conducted online with no identifying information to further protect anonymity.	
I have been informed that the data will be destroyed upon completion of the study.	
I acknowledge that some of the data collected during this study may be looked at by some people at De Montfort University or from regulatory authorities concerned with education where it is related to my participation this study. Moreover, I give consent for such individuals to be allowed access to my responses.	
I have been given the opportunity to request both the information sheet and this consent form in Arabic. إذ ترغب الحصول على نسخة باللغة العربية من جميع المستندات يمكنك طلب ذلك من الباحث	

With knowledge of the above-stated issues, I agree to participate in this study.

I agree to future contact by the researchers if my responses reveal interesting findings or for cross reference purposes. ☐ Yes ☐ No

If answered yes, the suitable method of being contacted is:

☐ Telephone ……☐ email ……

Participant Name:			
Participant Signature:		Date	

Senior Questionnaire

Dear Senior,

As you have been informed, this study aims to understand both the relationship and cloud factors within the relationship between the government and the cloud service provider that may have an impact on government adoption of the public cloud. As part of achieving this aim the researcher needs you to answer questions about the relationship you have with the provider and cloud concerns you have.

Your anonymity is guaranteed and you have the right to withdraw from the study at any time.

Please try to complete all of the questions. If you have any questions please feel free to contact the researcher. Contact details are provided below.

I would like to thank you for your invaluable contribution to the study.

Please tick the appropriate boxes ☐

Waleed Al Ghanim (PhD Researcher)

Faculty of Technology

De Montfort University

49 Oxford Street, Innovation Centre, LE1 5XY, Leicester, UK

P10003240@myemail.dmu.ac.uk

TEL: UK +44 7593042025

KSA +966555111598

Number	**Question** **1. Strongly Disagree 2. Disagree 3. Neutral 4. Agree 5. Strongly Agree**	**1**	**2**	**3**	**4**	**5**
TRUST DOMAIN						
Q1	You trust your CSP					
QUESTION 2A GOVERNANCE						
Q2A	In the relationship with the CSP you trust them in relation to governance					
Q2A 1-8	**You trust the CSP in relation to the following governance issues:**					
Q2A 1	Your need to have knowledge and control over data and processes					
Q2A 2	Assurance about other cloud tenants					
Q2A 3	Knowledge and control over third party issues					
Q2A 4	Clarity of roles and responsibilities					
Q2A 5	Dynamic SLA					
Q2A 6	Control and knowledge of CSP employees					
Q2A 7	Auditing and measuring of CSP					
Q2A 8	Governance during migration					
QUESTION 2B COMPLIANCE						
Q2B	In the relationship with the CSP you trust them in relation to compliance					
Q2B 1-8	**You trust the CSP in relation to the following compliance issues:**					
Q2B 1	Continuous auditing and assessment					

Q2B 2	Clarity and confidence about jurisdiction					
Q2B 3	Data management					
Q2B 4	Roles and responsibilities for compliance					
Q2B 5	Security and privacy					
Q2B 6	CSP ability to be compliant					
Q2B 7	Data location					
Q2B 8	Compliance when migrating					
QUESTION 2C SECURITY AND PRIVACY						
Q2C	In the relationship with the CSP you trust them in relation to compliance					
Q2C 1-7	**You trust the CSP in relation to the following security and privacy issues:**					
Q2C 1	Security related to third parties					
Q2C 2	Monitoring of policy adherence					
Q2C 3	Sufficient involvement in security					
Q2C 4	Tailored security and privacy policy					
Q2C 5	General security / privacy provision					
Q2C 6	Clarity of roles and responsibilities					
Q2C 7	Assurance regarding CSP employees					
QUESTION 2D PERFORMANCE AND OFFERING						
Q2D	In the relationship with the CSP you trust them in relation to performance and offering					
Q2D 1-9	**You trust the CSP in relation to the following performance and offering issues:**					

Q2D 1	Customisable cloud environment					
Q2D 2	Dynamic / flexible SLA					
Q2D 3	Continues monitoring of performance					
Q2D 4	Meet government specific requirements					
Q2D 5	Additional specialised staff for government needs					
Q2D 6	Back up and recovery					
Q2D 7	Sufficient support lifecycle					
Q2D 8	Sufficient notice of disruption					
Q2D 9	End of relationship					
RISK DOMAIN						
Q3	In your relationship with the CSP you do not perceive a risk					
QUESTION 4A GOVERNANCE						
Q4A	When engaging in the relationship with the CSP you do not perceive a risk in relation to governance					
Q4A 1-8	**In the relationship with the CSP you do not perceive a governance risk in relation to the following:**					
Q4A 1	Your need to have knowledge and control over data and processes					
Q4A 2	Assurance about other cloud tenants					
Q4A 3	Knowledge and control over third party issues					
Q4A 4	Clarity of roles and responsibilities					
Q4A 5	Dynamic SLA					
Q4A 6	Control and knowledge of CSP employees					

Q4A 7	Auditing and measuring of CSP					
Q4A 8	Governance during migration					
QUESTION 4B COMPLIANCE						
Q4B	When engaging in the relationship with the CSP you do not perceive a risk in relation to compliance					
Q4B 1-8	**In the relationship with the CSP you do not perceive a compliance risk in relation to the following:**					
Q4B 1	Continuous auditing and assessment					
Q4B 2	Clarity and confidence about jurisdiction					
Q4B 3	Data management					
Q4B 4	Roles and responsibilities for compliance					
Q4B 5	Security and privacy					
Q4B 6	CSP ability to be compliant					
Q4B 7	Data location					
Q4B 8	Compliance when migrating					
QUESTION 4C SECURITY AND PRIVACY						
Q4C	When engaging in the relationship with the CSP you do not perceive a risk in relation to security and privacy					
Q4C 1-7	**In the relationship with the CSP you do not perceive a security and privacy risk in relation to the following:**					
Q4C 1	Security related to third parties					
Q4C 2	Monitoring of policy adherence					
Q4C 3	Sufficient involvement in security					
Q4C 4	Tailored security and privacy policy					

Q4C 5	General security / privacy provision					
Q4C 6	Clarity of roles and responsibilities					
Q4C 7	Assurance regarding CSP employees					
QUESTION 4D PERFORMANCE AND OFFERING						
Q4D	When engaging in the relationship with the CSP you do not perceive a risk in relation to performance and offering					
Q4D 1-9	**In the relationship with CSP you do not perceive a performance and offering risk in relation to the following:**					
Q4D 1	Customisable cloud environment					
Q4D 2	Dynamic / flexible SLA					
Q4D 3	Continues monitoring of performance					
Q4D 4	Meet government specific requirements					
Q4D 5	Additional specialised staff for government needs					
Q4D 6	Back up and recovery					
Q4D 7	Sufficient support lifecycle					
Q4D 8	Sufficient notice of disruption					
Q4D 9	End of relationship					
Negotiation (Specify Requirements)						
Q5	You can effectively specify your requirements					
QUESTION 6A GOVERNANCE						
Q6A 1-8	**You feel can effectively specify your governance requirements in relation to the following:**					
Q6A 1	Your need to have knowledge and control over data and processes					

Q6A 2	Assurance about other cloud tenants					
Q6A 3	Knowledge and control over third party issues					
Q6A 4	Clarity of roles and responsibilities					
Q6A 5	Dynamic SLA					
Q6A 6	Control and knowledge of CSP employees					
Q6A 7	Auditing and measuring of CSP					
Q6A 8	Governance during migration					
QUESTION 6B COMPLIANCE						
Q6B	In the relationship with the CSP you are able to specify compliance requirements					
Q6B	**You can effectively specify your compliance requirements in relation to the following:**					
Q6B 1	Continuous auditing and assessment					
Q6B 2	Clarity and confidence about jurisdiction					
Q6B 3	Data management					
Q6B 4	Roles and responsibilities for compliance					
Q6B 5	Security and privacy					
Q6B 6	CSP ability to be compliant					
Q6B 7	Data location					
Q6B 8	Compliance when migrating					
QUESTION 6C SECURITY AND PRIVACY						
Q6C	In the relationship with the CSP you are able to specify security and privacy requirements					
Q6C 1-7	**You can effectively specify your security and privacy requirements in**					

	relation to the following:					
Q6C 1	Security related to third parties					
Q6C 2	Monitoring of policy adherence					
Q6C 3	Sufficient involvement in security					
Q6C 4	Tailored security and privacy policy					
Q6C 5	General security / privacy provision					
Q6C 6	Clarity of roles and responsibilities					
Q6C 7	Assurance regarding CSP employees					
QUESTION 6D PERFORMANCE AND OFFERING						
Q6D	In the relationship with the CSP you are able to specify performance and offering requirements					
Q6D 1-9	**You can effectively specify your performance and offering requirements in relation to the following:**					
Q6D 1	Customisable cloud environment					
Q6D 2	Dynamic / flexible SLA					
Q6D 3	Continues monitoring of performance					
Q6D 4	Meet government specific requirements					
Q6D 5	Additional specialised staff for government needs					
Q6D 6	Back up and recovery					
Q6D 7	Sufficient support lifecycle					
Q6D 8	Sufficient notice of disruption					
Q6D 9	End of relationship					
Negotiation (Understand Requirements)						

Q7	Your CSP understands your requirements					
QUESTION 8A GOVERNANCE						
Q8A	In the relationship with your CSP, they understand your governance requirements					
Q8A 1-8	**Your CSP understands your governance requirements in relation to the following:**					
Q8A 1	Your need to have knowledge and control over data and processes					
Q8A 2	Assurance about other cloud tenants					
Q8A 3	Knowledge and control over third party issues					
Q8A 4	Clarity of roles and responsibilities					
Q8A 5	Dynamic SLA					
Q8A 6	Control and knowledge of CSP employees					
Q8A 7	Auditing and measuring of CSP					
Q8A 8	Governance during migration					
QUESTION 8B COMPLIANCE						
Q8B	In the relationship with your CSP, they understand your compliance requirements					
Q8B 1-8	**Your CSP understands your compliance requirements in relation to the following:**					
Q8B	Continuous auditing and assessment					
Q8B	Clarity and confidence about jurisdiction					
Q8B	Data management					
Q8B	Roles and responsibilities for compliance					

Q8B	Security and privacy					
Q8B	CSP ability to be compliant					
Q8B	Data location					
Q8B	Compliance when migrating					
QUESTION 8C SECURITY AND PRIVACY						
Q8C	In the relationship with your CSP, they understand your security and privacy requirements					
Q8C 1-7	**Your CSP understands your security and privacy requirements in relation to the following:**					
Q8C 1	Security related to third parties					
Q8C 2	Monitoring of policy adherence					
Q8C 3	Sufficient involvement in security					
Q8C 4	Tailored security and privacy policy					
Q8C 5	General security / privacy provision					
Q8C 6	Clarity of roles and responsibilities					
Q8C 7	Assurance regarding CSP employees					
QUESTION 8D PERFORMANCE AND OFFERING						
Q8D	In the relationship with your CSP, they understand your performance and offering requirements					
Q8D 1-9	**The CSP understands your performance and offering requirements in relation to the following:**					
Q8D 1	Customisable cloud environment					
Q8D 2	Dynamic / flexible SLA					
Q8D 3	Continues monitoring of performance					

Q8D 4	Meet government specific requirements					
Q8D 5	Additional specialised staff for government needs					
Q8D 6	Back up and recovery					
Q8D 7	Sufficient support lifecycle					
Q8D 8	Sufficient notice of disruption					
Q8D 9	End of relationship					
Negotiation (General)						
Q9	You can negotiate with your CSP					
QUESTION 10A GOVERNANCE						
Q10A 1-8	In the relationship with your CSP you can negotiate your governance requirements					
Q10A	**You can negotiate your governance requirements in relation to the following:**					
Q10A 1	Your need to have knowledge and control over data and processes					
Q10A 2	Assurance about other cloud tenants					
Q10A 3	Knowledge and control over third party issues					
Q10A 4	Clarity of roles and responsibilities					
Q10A 5	Dynamic SLA					
Q10A 6	Control and knowledge of CSP employees					
Q10A 7	Auditing and measuring of CSP					
Q10A 8	Governance during migration					
QUESTION 10B COMPLIANCE						

Q10B	In the relationship with your CSP you can negotiate your compliance requirements					
Q10B 1-8	**You can negotiate your compliance requirements in relation to the following:**					
Q10B 1	Continuous auditing and assessment					
Q10B 2	Clarity and confidence about jurisdiction					
Q10B 3	Data management					
Q10B 4	Roles and responsibilities for compliance					
Q10B 5	Security and privacy					
Q10B 6	CSP ability to be compliant					
Q10B 7	Data location					
Q10B 8	Compliance when migrating					
QUESTION 10C SECURITY AND PRIVACY						
Q10C	In the relationship with your CSP you can negotiate your security and privacy requirements					
Q10C 1-7	**You can negotiate your security and privacy requirements in relation to the following:**					
Q10C 1	Security related to third parties					
Q10C 2	Monitoring of policy adherence					
Q10C 3	Sufficient involvement in security					
Q10C 4	Tailored security and privacy policy					
Q10C 5	General security / privacy provision					
Q10C 6	Clarity of roles and responsibilities					

Q10C 7	Assurance regarding CSP employees					
QUESTION 10D PERFORMANCE AND OFFERING						
Q10D	In the relationship with your CSP you can negotiate your performance and offering requirements					
Q10D 1-9	**You can negotiate your performance and offering requirements in relation to the following:**					
Q10D 1	Customisable cloud environment					
Q10D 2	Dynamic / flexible SLA					
Q10D 3	Continues monitoring of performance					
Q10D 4	Meet government specific requirements					
Q10D 5	Additional specialised staff for government needs					
Q10D 6	Back up and recovery					
Q10D 7	Sufficient support lifecycle					
Q10D 8	Sufficient notice of disruption					
Q10D 9	End of relationship					
COLLABORATION DOMAIN						
Q 11	You can effectively collaborate with your CSP					
QUESTION 12A GOVERNANCE						
Q12A	You can effectively collaborate with your CSP about governance					
Q12A 1-8	**You can effectively collaborate with your CSP about the following governance issues:**					
Q12A 1	Your need to have knowledge and control over data and processes					

Q12A 2	Assurance about other cloud tenants					
Q12A 3	Knowledge and control over third party issues					
Q12A 4	Clarity of roles and responsibilities					
Q12A 5	Dynamic SLA					
Q12A 6	Control and knowledge of CSP employees					
Q12A 7	Auditing and measuring of CSP					
Q12A 8	Governance during migration					
QUESTION 12B COMPLIANCE						
Q12B	You can effectively collaborate with your CSP about compliance					
Q12B 1-8	**You can effectively collaborate with your CSP about the following compliance issues:**					
Q12B 1	Continuous auditing and assessment					
Q12B 2	Clarity and confidence about jurisdiction					
Q12B 3	Data management					
Q12B 4	Roles and responsibilities for compliance					
Q12B 5	Security and privacy					
Q12B 6	CSP ability to be compliant					
Q12B 7	Data location					
Q12B 8	Compliance when migrating					
QUESTION 12C SECURITY AND PRIVACY						
Q12C	You can effectively collaborate with your CSP about security and privacy					

Q12C 1-7	**You can effectively collaborate with your CSP about the following security and privacy issues:**					
Q12C 1	Security related to third parties					
Q12C 2	Monitoring of policy adherence					
Q12C 3	Sufficient involvement in security					
Q12C 4	Tailored security and privacy policy					
Q12C 5	General security / privacy provision					
Q12C 6	Clarity of roles and responsibilities					
Q12C 7	Assurance regarding CSP employees					
QUESTION 12D PERFORMANCE AND OFFERING						
Q12D	You can effectively collaborate with your CSP about performance and offering					
Q12D 1-9	**You can effectively collaborate with your CSP about the following performance and offering issues:**					
Q12D 1	Customisable cloud environment					
Q12D 2	Dynamic / flexible SLA					
Q12D 3	Continues monitoring of performance					
Q12D 4	Meet government specific requirements					
Q12D 5	Additional specialised staff for government needs					
Q12D 6	Back up and recovery					
Q12D 7	Sufficient support lifecycle					
Q12D 8	Sufficient notice of disruption					
Q12D 9	End of relationship					

COLLABORATION (effectively communicate)						
Q13	You can effectively communicate with your CSP					
QUESTION 14A GOVERNANCE						
Q14A	You can effectively communicate with your CSP about governance					
Q14A 1-8	**You can effectively communicate with your CSP about the following governance issues:**					
Q14A 1	Your need to have knowledge and control over data and processes					
Q14A 2	Assurance about other cloud tenants					
Q14A 3	Knowledge and control over third party issues					
Q14A 4	Clarity of roles and responsibilities					
Q14A 5	Dynamic SLA					
Q14A 6	Control and knowledge of CSP employees					
Q14A 7	Auditing and measuring of CSP					
Q14A 8	Governance during migration					
QUESTION 14B COMPLIANCE						
Q14B	You can effectively communicate with your CSP about compliance					
Q14B 1-8	**You can effectively communicate with your CSP about the following compliance issues:**					
Q14B 1	Continuous auditing and assessment					
Q14B 2	Clarity and confidence about jurisdiction					
Q14B 3	Data management					

Q14B 4	Roles and responsibilities for compliance					
Q14B 5	Security and privacy					
Q14B 6	CSP ability to be compliant					
Q14B 7	Data location					
Q14B 8	Compliance when migrating					
QUESTION 14C SECURITY AND PRIVACY						
Q14C	You can effectively communicate with your CSP about security and privacy					
Q14C 1-7	**You can effectively communicate with your CSP about the following security and privacy issues:**					
Q14C 1	Security related to third parties					
Q14C 2	Monitoring of policy adherence					
Q14C 3	Sufficient involvement in security					
Q14C 4	Tailored security and privacy policy					
Q14C 5	General security / privacy provision					
Q14C 6	Clarity of roles and responsibilities					
Q14C 7	Assurance regarding CSP employees					
QUESTION 14D PERFORMANCE AND OFFERING						
Q14D	You can effectively communicate with your CSP about performance and offering					
Q14D 1-9	**You can effectively communicate with your CSP about the following performance and offering issues:**					
Q14D 1	Customisable cloud environment					
Q14D 2	Dynamic / flexible SLA					

Q14D 3	Continuos monitoring of performance					
Q14D 4	Meet government specific requirements					
Q14D 5	Additional specialised staff for government needs					
Q14D 6	Back up and recovery					
Q14D 7	Sufficient support lifecycle					
Q14D 8	Sufficient notice of disruption					
Q14D 9	End of relationship					
REPUTATION DOMAIN						
Q15	You have sufficient information about your CSP					
QUESTION 16A GOVERNANCE						
Q16A	You have sufficient information about your CSP regarding governance					
Q16A 1-9	**You have sufficient information about your CSP regarding the following governance issues:**					
Q16A 1	Your need to have knowledge and control over data and processes					
Q16A 2	Assurance about other cloud tenants					
Q16A 3	Knowledge and control over third party issues					
Q16A 4	Clarity of roles and responsibilities					
Q16A 5	Dynamic SLA					
Q16A 6	Control and knowledge of CSP employees					
Q16A 7	Auditing and measuring of CSP					
Q16A 8	Governance during migration					
QUESTION 16B COMPLIANCE						

Q16B	You have sufficient information about your CSP regarding compliance					
Q16B 1-8	**You have sufficient information about your CSP regarding the following compliance issues:**					
Q16B 1	Continuous auditing and assessment					
Q16B 2	Clarity and confidence about jurisdiction					
Q16B 3	Data management					
Q16B 4	Roles and responsibilities for compliance					
Q16B 5	Security and privacy					
Q16B 6	CSP ability to be compliant					
Q16B 7	Data location					
Q16B 8	Compliance when migrating					
QUESTION 16C SECURITY AND PRIVACY						
Q16C	You have sufficient information about your CSP regarding security and privacy					
Q16C 1-7	**You have sufficient information about your CSP regarding the following security and privacy issues:**					
Q16C 1	Security related to third parties					
Q16C 2	Monitoring of policy adherence					
Q16C 3	Sufficient involvement in security					
Q16C 4	Tailored security and privacy policy					
Q16C 5	General security / privacy provision					
Q16C 6	Clarity of roles and responsibilities					
Q16C 7	Assurance regarding CSP employees					

QUESTION 16D PERFORMANCE AND OFFERING						
Q16D	You have sufficient information about your CSP regarding performance and offering:					
Q16D 1-9	**You have sufficient information about your CSP regarding the following performance and offering issues:**					
Q16D 1	Customisable cloud environment					
Q16D 2	Dynamic / flexible SLA					
Q16D 3	Continues monitoring of performance					
Q16D 4	Meet government specific requirements					
Q16D 5	Additional specialised staff for government needs					
Q16D 6	Back up and recovery					
Q16D 7	Sufficient support lifecycle					
Q16D 8	Sufficient notice of disruption					
Q16D 9	End of relationship					
REPUTATION						
Q17	You perceive a positive reputation of your CSP					
QUESTION 18A GOVERNANCE						
Q18A	You perceive a positive reputation in relation to governance					
Q18A 1-8	**You perceive a positive reputation in relation to the following governance areas:**					
Q18A 1	Your need to have knowledge and control over data and processes					
Q18A 2	Assurance about other cloud tenants					
Q18A 3	Knowledge and control over third party issues					

Q18A 4	Clarity of roles and responsibilities					
Q18A 5	Dynamic SLA					
Q18A 6	Control and knowledge of CSP employees					
Q18A 7	Auditing and measuring of CSP					
Q18A 8	Governance during migration					
QUESTION 18B COMPLIANCE						
Q18B	You perceive a positive reputation in relation to compliance					
Q18B 1-8	**You perceive a positive reputation in relation to the following compliance areas:**					
Q18B 1	Continuous auditing and assessment					
Q18B 2	Clarity and confidence about jurisdiction					
Q18B 3	Data management					
Q18B 4	Roles and responsibilities for compliance					
Q18B 5	Security and privacy					
Q18B 6	CSP ability to be compliant					
Q18B 7	Data location					
Q18B 8	Compliance when migrating					
QUESTION 18C SECURITY AND PRIVACY						
Q18C	You perceive a positive reputation in relation to security and privacy					
Q18C 1-7	**You perceive a positive reputation in relation to the following security and privacy areas:**					
Q18C 1	Security related to third parties					

Q18C 2	Monitoring of policy adherence					
Q18C 3	Sufficient involvement in security					
Q18C 4	Tailored security and privacy policy					
Q18C 5	General security / privacy provision					
Q18C 6	Clarity of roles and responsibilities					
Q18C 7	Assurance regarding CSP employees					
QUESTION 18D PERFORMANCE AND OFFERING						
Q18D	You perceive a positive reputation in relation to performance and offering					
Q18D 1-9	**You perceive a positive reputation in relation to the following performance and offering areas:**					
Q18D 1	Customisable cloud environment					
Q18D 2	Dynamic / flexible SLA					
Q18D 3	Continuos monitoring of performance					
Q18D 4	Meet government specific requirements					
Q18D 5	Additional specialised staff for government needs					
Q18D 6	Back up and recovery					
Q18D 7	Sufficient support lifecycle					
Q18D 8	Sufficient notice of disruption					
Q18D 9	End of relationship					

Relationship and Cloud Factors Affecting Government Confidence in the Public Cloud

Participant Information Sheet (Interview)

Dear participant,

I would like you to take part in a study conducted by a researcher at De Montfort University in the United Kingdom.

The study is investigating the relationship between the government as a customer and providers of the public cloud and how this relationship affects government confidence in deploying sensitive data and critical systems in the public cloud.

As your position means that you are involved in this relationship, it is felt that you can provide data that is both relevant and useful to this study.

Participation in this study is voluntary and will involve a semi-structured interview, which will take approximately 1 hour.

Participation is voluntary and you have the right to withdraw from the study at any point. If you do chose to withdraw all of the gained identifiable data will be destroyed, however, if the data has been anonymised then it will not be destroyed because identification of the origin of the data will not be possible.

Data from the interviews may be used in publications associated this study.

Privacy, confidentiality and anonymity will be assured by the researcher.

The information that is gained in this research will not be used for other research and will only be used for purposes informed here.

Data will be kept in a secure location and can only be accessed by the researcher and the participant will be able to request their data at any time throughout the research.

If there are any questions regarding this research please contact the researcher at:
P10003240@myemail.dmu.ac.uk

Waleed Al Ghanim (PhD Researcher)

Faculty of Technology, *De Montfort University*, 49 Oxford Street, Innovation Centre, LE1 5XY, Leicester, UK

TEL: +44 7593042025

Consent form for interview

Please complete the following form by signing initials in the corresponding boxes:

Issue	Participant's initial
I have read the information provided in the participant information sheet	
I have been given the opportunity to ask questions about the study, answers were satisfactory and I was provided with additional information when requested.	
I understand that participation is voluntary and I have the right to withdraw from the study at any time and that my data will be destroyed.	
I am aware that data from the interview may be used in publications associated with this study, and that all of the data will be anonymised.	
I have been informed that the data will be kept in a secure location and only used for research purposes. I also know that at any time I can request a copy of the data.	
I have been informed that the data will be destroyed upon completion of the study.	
I acknowledge that data collected may be looked at by some people at De Montfort University. Moreover, I give consent for such individuals to be allowed access to my responses.	

I agree to future contact by the researchers if my responses reveal interesting findings or for cross reference purposes. ☐ Yes ☐ No

If answered yes, the suitable method of being contacted is:

☐ Telephone ……☐ email ……

With knowledge and consent of the above issues, I agree to participate in this study.

Participant Name:			
Participant Signature:		Date	

Interview questions

1. *Do you currently have plans to use the public cloud for sensitive data and critical systems?*
2. *What are the concerns that you have about the public cloud?*
3. *How is your relationship with your CSP?*
4. *Do you trust your CSP?*
5. *In relation to your CSP, do you perceive any risks?*
6. *Are you able to negotiate effectively with your CSP?*
7. *Do you feel that concerns can be resolved through the relationship with the CSP?*
8. *Does your CSP accommodate all your needs?*
9. *Are you kept informed by your CSP?*
10. *How do you collaborate with you CSP?*
11. *How involved are you with the provision of the public cloud as a service?*
12. *Do you perceive a positive reputation of your CSP?*